On Solvable Septics

Lau Jing Feng

A THESIS SUBMITTED
FOR THE DEGREE OF MASTER OF SCIENCE.

Supervisor : A/P. Lang Mong Lung

Department of Mathematics
National University of Singapore
2004

Acknowledgements

I am grateful to my supervisor A/P Lang Mong Lung for his patient guidance and for giving me this the opportunity to self propose my own thesis topic. He has never fail to inspire me and keep my interest in Mathematics 'alive' despite all the disappointment and unhappiness I face in 2002 and 2003. I also wish to thank Sze Ling, Chee Peng and my sincere friends in Gakkai for encouraging me to move on during my most difficult time in 2003.

Contents

Summary

This thesis seeks to examine the computational aspects in solving solvable septics.

An account of the historical background is provided in Chapter 1.

In Chapter 2, the approach in [D] is generalized to lay down the qualitative theory behind solving polynomials of an arbitrary prime degree p. The main problem is broken down into four points of consideration and the results and drawbacks of applying Dummit's approach to each of the four points are outlined.

Chapter 3 presents the approach of Lagrange resolvents to solving solvable septics. Technicalities faced in adopting this methodology are highlighted and explicit calculations are performed to solve for two roots of a particular septic polynomial associated to $\cos \frac{2\pi}{29}$.

Chapter 1

Introduction

The purpose of this chapter is to expound on what has been done on the subject of solving polynomials in one variable by expressing the roots in radicals. Due to the technicalities involved, we shall omit the details and present the main ideas and results.

1.1 Historical Development

1. The Babylonians, Greeks and Arabs were known to be the first to solve quadratic equations. Motivated by plane geometry, the method of "completing the square" yields the solution

$$x = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

to the quadratic equation

$$x^2 + ax + b = 0 \ \ (\text{cf. } [\text{T}])\,.$$

2. The algebraic solution of $x^3+mx = n$ was first obtained around 1515 by Scipione del Ferro, Professor of Mathematics in Bologna. In 1535, Antonio Mario Fior, a student of Scipione del Ferro challenged Tartaglia, who had previously attempted to solve certain types of cubic equations in a problem-solving contest to solve about thirty problems on equations of the form $x^3 + mx = n$. Tartaglia succeeded in finding the solution to win the challenge and when news of this reached Jerôme Cardan, the latter asked Tartaglia to reveal his solution. Cardan published all these solutions in his book Ars Magna which resulted into a bitter quarrel between Tartaglia and Cardan, the former claiming that

Cardan had solemnly sworn never to publish Tartaglia's solution, while the latter countered that there had never been any question of secrecy (cf. [E]). Using Cardan's method, the general cubic equation

$$x^3 + ax^2 + bx + c = 0$$

is reduced by the change of variable $y = x + \frac{a}{3}$ to the form

$$y^3 + py + q = 0$$

where

$$p = \frac{3b - a^2}{3} \text{ and } q = \frac{9c - 3ab + 2a^3}{27}\,.$$

Setting $y := u + v$, $3uv := -p$ and ω as a fixed primitive cube root of unity, the roots of the last cubic polynomial are

$$u + v\,,\ \omega y + \omega^2 z\,,\ \omega^2 y + \omega z$$

where

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}\,,\ v = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}\ \text{(cf. [DF])}\,.$$

Cardan's cubic formula led to the discovery of "Casus Irreducibilis", the impossibility of expressing the real roots of cubic equations in real radicals. Even though attempts to rewrite specific formulas to eliminate non-real complex numbers failed, they prompted greater understanding and usage of complex numbers (cf. [R2] and [I]).

3. The solution of quartic equations was found shortly after that of cubic equations. Cardan provided a method of solving such equations in the "Ars Magna" and he attributed it to his student Ludovico Ferrari (cf. [E] and [T]). For the general quartic equation

$$x^4 + ax^3 + bx^2 + cx + d = 0\,,$$

under the change of variable $y = x + \frac{a}{4}$ transforms the equation to

$$y^4 + py^2 + qy + r = 0$$

with

$$p = \frac{8b - 3a^2}{8}\,,\ q = \frac{8c - 4ab + a^3}{8}\,,\ r = \frac{256d - 64ac + 16a^2b - 3a^4}{256}\,.$$

Let the roots of $y^4 + py^2 + qy + r$ be y_1, y_2, y_3 and y_4. Define the resolvent cubic to be $x^3 - 2px^2 + (p^2 - 4r)x + q^2$ which has roots

$$\theta_1 = (y_1 + y_2)(y_3 + y_4)\,,\ \theta_2 = (y_1 + y_3)(y_2 + y_4)\,,\ \theta_3 = (y_1 + y_4)(y_2 + y_3)\,.$$

Then

$$y_1 = \tfrac{1}{2}(\sqrt{-\theta_1} + \sqrt{-\theta_2} + \sqrt{-\theta_3})\,,\ y_2 = \tfrac{1}{2}(\sqrt{-\theta_1} - \sqrt{-\theta_2} - \sqrt{-\theta_3})\,,$$

$$y_3 = \tfrac{1}{2}(-\sqrt{-\theta_1} + \sqrt{-\theta_2} - \sqrt{-\theta_3})\,,\ y_4 = \tfrac{1}{2}(-\sqrt{-\theta_1} - \sqrt{-\theta_2} + \sqrt{-\theta_3})\,,$$

where $\sqrt{-\theta_1}\sqrt{-\theta_2}\sqrt{-\theta_3} = -q$ (cf. [DF]).

4. By introducing the Lagrange resolvent in 1770, Lagrange proposed another alternative method of solving cubic equations. Moreover, he showed that polynomials of degree five or more cannot be solved by the methods used for cubics and quartics. Assuming without justification that the radicals can be rationally expressed in terms of the roots of the initial equation, Paolo Ruffini gave a proof on the impossibility to solve general equations of degree higher than 4 in his book General Theory of Equations (cf. [PS]). It was not till 1826 that Niels Henrik Abel provided the first complete proof on the unsolvability of the general equation of degree higher than 4. From the theoretical viewpoint, it was Evariste Galois who made the major breakthrough by drawing correspondence between equations and groups. With subsequent refinements by Ludwig Sylow in 1871 and Emil Artin in 1938 on Galois's results which culminated into what is known today as Galois Theory, these led to the development of the modern theory of algebraic equations (cf. [V]). Among these lies Galois epoch-making theorem which asserts that the solvability by radicals of a polynomial is equivalent to solvability of its Galois group.

5. Some progress were made in the direction of solving algebraic equations using elliptic functions. It first started out in 1829 with Carl Gustav Jacobi studying modular equations for elliptic functions which are fundamental for Hermite's solution of quintics in 1858. This is subsequently followed by the advancements of Camille Jordan in 1870 who showed that algebraic equations of any degree can be solved in terms of modular functions and Ferdinand von Lindemann expressing the roots of an arbitrary polynomial in terms of theta functions (cf. [V]).

1.2 Recent Advancements

1. Having showed that every quintic can be transformed to the form

$$x^5 + ax + b = 0 \tag{1.2.1}$$

by Erland Samuel Bring and George Birch Jerrad in 1786 and 1834 respectively (cf. [V]), Spearman and Williams [SW] showed that an irreducible quintic of the form (1.2.1) having rational coefficients is solvable by radicals if and only if there exist rational numbers $\epsilon = \pm 1$, $c \geq 0$ and $e \neq 0$ such that

$$a = \frac{5e^4(3 - 4\epsilon c)}{c^2 + 1}\,,\; b = \frac{-4e^5(11\epsilon + 2c)}{c^2 + 1}\,.$$

When this is the case, the roots are given by

$$x_j = e(\omega^j u_1 + \omega^{2j} u_2 + \omega^{3j} u_3 + \omega^{4j} u_4)$$

where

$$u_1 = \left(\frac{v_1^2 v_3}{D^2}\right)^{1/5},\; u_2 = \left(\frac{v_3^2 v_4}{D^2}\right)^{1/5},\; u_3 = \left(\frac{v_2^2 v_1}{D^2}\right)^{1/5},\; u_4 = \left(\frac{v_4^1 v_2}{D^2}\right)^{1/5},$$

$$v_1 = \sqrt{D} + \sqrt{D - \epsilon\sqrt{D}}\,,\; v_2 = -\sqrt{D} - \sqrt{D + \epsilon\sqrt{D}}\,,$$

$$v_3 = -\sqrt{D} + \sqrt{D + \epsilon\sqrt{D}}\,,\; v_4 = \sqrt{D} - \sqrt{D - \epsilon\sqrt{D}}\,,\; D = c^2 + 1\,,$$

and ω is a fixed primitive 5th root of unity.

2. David Dummit [D] and (independently) Sigeru Kobayashi and Hiroshi Nakagawa [KN] gave methods for finding the roots of a general solvable quintic in radicals. Dummit employed techniques from function field theory to give an explicit criterion for the solvability of a quintic in terms of the existence of a rational root θ of a certain sextic resolvent. Denoting the function field $\mathbb{Q}(x_1, \cdots, x_5)$ as K and the Frobenius group of degree 5 by F_{20}, the rational coefficients of certain invariants are viewed as elements of the fixed field $K^{F_{20}}$ which is of degree 6 over K^{S_5} so that they can be written as a linear combination of 1, θ, $\cdots$, θ^5 and calculated by solving linear systems of 6 equations in 6 unknowns. Not only are these invariants used to compute other intermediate invariants, they are also used to determine uniqueness of some other invariants up to some permutation and the choice of the $5th$ root to take in order to obtain each of the Lagrange resolvents.

3. Even with the advent of modern computers, it took 9 years before the case for solvable degree 6 polynomials was settled by Thomas R. Hagedorn [H] in 2000. In [H], Hagedorn discusses the 16 transitive subgroups of S_6 up to isomorphism and information about the Galois group of the original sextic $f(x)$ is obtained by factoring resolvents of degree 2, 10 and 15 and computing the discriminant. Depending on whether the Galois group of $f(x)$ is a subgroup of G_{48} or G_{72}, the author designed algorithms which uses the rational roots of the resolvents of degree 10 and 15 to define new resolvent polynomials and other polynomials. The roots of these resolvents are used to define other polynomials and Galois resolvents and the previous step are repeated until enough polynomials are defined so that the Galois group and the roots of $f(x)$ can be calculated.

Chapter 2

Solving Solvable Polynomials of prime degree

In this chapter, we shall identify the irreducible polynomials of prime degree p over $\mathbb{Q}$ which are solvable by radicals and outline both the qualitative theory and computational aspects in solving polynomials of prime degree via the method of Lagrange resolvents.

2.1 Solvable Galois Groups of irreducible polynomials of prime degree p

In this section, we shall present a classical result which was first proved by Galois that provides a necessary and sufficient condition for an irreducible polynomial of prime degree p to be solvable by radicals.

We begin with some terminology and notations.

Definition 2.1.1. *Let G be a group. A G-set X is transitive if for every x, $y \in X$, there exists $\sigma \in G$ with $y = \sigma x$. In this case, the group G is said to act transitively on X.*

Definition 2.1.2. *A group G is solvable if it has a normal series*

$$\{1_G\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

whose factors G_i/G_{i-1} are abelian for all $1 \leq i \leq n$.

Definition 2.1.3. *If X is a G-set, then the stabilizer of x, denoted by G_x, is the subgroup*

$$G_x := \{g \in G : gx = x\} \leq G\,.$$

Next, we state the following result from [R1] without proof.

Proposition 2.1.4. *Let X be a transitive G-set, and let x, $y \in X$. If $gx = y$ for some $g \in G$, then $G_y = g\,G_x\,g^{-1}$.*

Lemma 2.1.5. *Let X be a transitive G-set and $\alpha \in X$ be arbitrary. If N is a normal subgroup of G contained in G_α, then N is a subgroup of*

$$\bigcap_{\beta \in X} G_\beta\,.$$

Moreover, if G also acts faithfully on X, then G_α contains no non-trivial normal subgroups of G.

Proof. If N is normal in G,

$$N = \bigcap_{g \in G} gNg^{-1} \subseteq \bigcap_{\substack{g \in G \\ g(\alpha) = \beta}} gNg^{-1} \subseteq \bigcap_{\beta \in X} G_\beta$$

by Proposition 2.1.4. Hence the conclusion follows. □

Before we state and prove the main result of this section as promised, we will need to introduce some new notation. We shall denote the cyclic group of order n as $\mathbb{Z}_n$, the dihedral group of order $2n$ as D_{2n}, the semidirect product of K by Q as $K \rtimes Q$ and the Frobenius group of degree p as $F_{p(p-1)}$ or $\mathbb{Z}_p \rtimes \mathbb{Z}_{p-1}$.

Theorem 2.1.6. (*Galois*) *An irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree p is solvable by radicals if and only if its Galois group is isomorphic to a transitive subgroup of $\mathbb{Z}_p \rtimes \mathbb{Z}_{p-1}$, the Frobenius group of degree p.*

Proof. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p with Galois group G. Suppose G is a subgroup of $\mathbb{Z}_p \rtimes \mathbb{Z}_{p-1}$. Since $\mathbb{Z}_p \rtimes \mathbb{Z}_{p-1}$ is solvable and every subgroup of a solvable group is itself solvable, G is solvable and so $f(x)$ is solvable by radicals. Conversely, suppose $f(x)$ is solvable by radicals. Thus G is solvable. Let $G^{(n-1)}$ be the last nontrivial subgroup in the normal series for G. Then $G^{(n-1)}$ as a solvable minimal normal subgroup of G have no non-trivial proper characteristic subgroups and so must be an elementary abelian p-group. Since G is isomorphic to a subgroup of S_p, $G^{(n-1)}$ is isomorphic to $\mathbb{Z}_p$. Denoting the image of $G^{(n-1)}$ in S_p as H, $G^{(n-1)}$ being normal in G implies that G is isomorphic to a transitive subgroup of $N_{S_p}(H)$. □

From the above theorem, we deduce the following corollary.

Corollary 2.1.7. *Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 7. Then $f(x)$ is solvable by radicals if and only if its Galois group is a transitive subgroup of F_{42}. In particular, if G is the Galois group of $f(x)$, then G is isomorphic to either $\mathbb{Z}_7$, D_{14}, $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$ or F_{42}.*

2.2 Fixed Fields of the Frobenius group $F_{p(p-1)}$

In this section, we shall analyze closely the relationship between the intermediate fields of $\mathbb{Q}$, the splitting field of a given solvable irreducible polynomial $f(x)$ of prime degree p and the radical extension obtained by adjoining a primitive pth root of unity. Since all such polynomials have Galois groups which are isomorphic to transitive subgroups of $F_{p(p-1)}$, we shall be working mainly with the function field $\mathbb{Q}(x_1, \cdots, x_p)$ over the fixed field of $F_{p(p-1)}$. For convenience, we shall denote the normal subgroup of $F_{p(p-1)}$ which is isomorphic to $\mathbb{Z}_p$ by N and its complement which is isomorphic to $\mathbb{Z}_{p-1}$ by C. We let σ and τ denote fixed generators of N and C respectively.

Definition 2.2.1. *Let p be an odd prime, $x_1, \cdots, x_p$ be p indeterminates over $\mathbb{Q}$,*

$$\Delta := \prod_{i<j}(x_i - x_j)$$

denote the fixed square root of the discriminant $D = \Delta^2$ and ζ be a fixed primitive pth root of unity. Take the nth symmetric function s_n of $x_1, x_2, \cdots, x_p$ as the sum of all products of the x_j's taken n at a time. Then for instance

$$s_1 := \sum_{j=1}^{p} x_j \quad \textit{and} \quad s_p := \prod_{j=1}^{p} x_j \,.$$

Define $K := \mathbb{Q}(x_1, \cdots, x_p)$, $k := \mathbb{Q}(s_1, \cdots, s_p)$, $F := K^{F_{p(p-1)}}$, $E := K^N$, $F' := E^{\langle \tau^2 \rangle}$ and $L := K(\zeta)$.

Proposition 2.2.2.

$$Gal(L/F) \cong F_{p(p-1)} \times \mathbb{Z}_p^* \,.$$

Proof. Since $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois with Galois group isomorphic to $\mathbb{Z}_p^*$ and $\mathbb{Q}(\zeta) \cap F = \mathbb{Q}$, the same conclusion holds for the extension $F(\zeta)/F$ by natural irrationalities. This together with the fact that K/F is Galois with $F_{p(p-1)}$ as Galois group implies our desired conclusion. □

Remark 2.2.3. Keeping Proposition 2.2.2 and our description of σ as the generator of N in mind, σ is defined to be the automorphism on L over k that permutes the set $\{x_1, \cdots, x_p\}$ cyclically. For our convenience, we shall denote σ by

$$\sigma := (1,\ 2, \cdots,\ p) \,.$$

(i). Recall that $F_{p(p-1)}$ is isomorphic to a semidirect product of N by C. Consequently we have a homomorphism $\phi : C \longrightarrow Aut(N)$ defined by $\phi(g) :\equiv \phi_g$ where for all $g \in C$, $a \in N$,

$$\phi_g(a) := gag^{-1}\,.$$

Note that $ker\phi$ is trivial because $C_{S_p}(\sigma) = N$. Hence ϕ as an injection from C to $Aut(N)$ with $|C| = |Aut(N)| = p-1$ must be an isomorphism. Therefore for any primitive root s of $\mathbb{Z}_p$, the map $\sigma \mapsto \sigma^s$ induces an automorphism of N of order $p-1$ which corresponds to a generator of C. In view of this, the automorphism

$$\tau := (2,\ s+1,\ s^2+1,\ \cdots,\ s^{p-2}+1)$$

acting trivially on constants is a generator of C.

(ii). We can deduce from σ, $\tau^2 \in A_p$ that $\Delta \in K^{N \rtimes \langle \tau^2|_K \rangle}$.

In the following result, we shall state without proof that $F_{p(p-1)}$ is maximal in S_p.

Proposition 2.2.4. *$F_{p(p-1)}$ is a maximal subgroup of S_p.*

Next we will determine all subgroups of $F_{p(p-1)}$ and among these subgroups identify those which are normal.

Proposition 2.2.5. *Let $G := \langle\sigma\rangle \rtimes \langle\tau\rangle$ be a Frobenius group acting on $X := \{1, 2, \cdots, p\}$. Denote by G_m the stabilizer of $m \in X$.*

(i). For each divisor d of $p-1$, $\langle\sigma\rangle \rtimes \langle\tau^{(p-1)/d}\rangle$ is the only subgroup of G of order pd.

(ii). $G_m \cap G_n = 1$ for $1 \le m, n \le p$, $m \ne n$.

(iii). G is the disjoint union of $G_1^*, \cdots, G_p^*$ and G'.

(iv). The collection $\{\, \langle\sigma\rangle \rtimes \langle\tau^{(p-1)/d}\rangle \,|\, d|(p-1)\,\}$ are precisely all the non-trivial normal subgroups of G.

(v). Let $H \ne 1$ be a subgroup of G_m. Then $N_G(H) = G_m$ and for each $0 \le i \le p-1$, $\sigma^i H \sigma^{-i} \subseteq G_{\sigma^i m}$ and H, $\sigma H \sigma^{-1}$, $\cdots$, $\sigma^{p-1} H \sigma$ are precisely all the distinct conjugates of H.

(vi). Every non-trivial subgroup H of order d dividing $p-1$ must be contained in some unique G_n. In particular, the subgroups G_1, G_2,$\cdots$, G_p are precisely all the distinct copies of $\mathbb{Z}_{p-1}$ in G.

Proof. (i). Let S be a subgroup of order pd. By Sylow's theorem, $\langle\sigma\rangle \subseteq S$. Hence $S/\langle\sigma\rangle$ is the unique cyclic subgroup of $G/\langle\sigma\rangle$ of order $(p-1)/d$. As a consequence, $S = \langle\sigma\rangle \rtimes \langle\tau^{(p-1)/d}\rangle$ by Correspondence theorem.

(ii). (ii) follows from the fact that elements in G fix at most 1 letter.

(iii). (ii) together with $N \cap G_n = 1$ for all $1 \leq n \leq p$ implies (iii).

(iv). Let A be a normal subgroup of G. Suppose that $\gcd(|A|, p) = 1$. Then $\langle\sigma\rangle \times A$ admits an element of order pk where $k > 1$, a contradiction. Thus $p||A|$ from which (iv) follows from (i).

(v). Suppose $p||N_G(H)|$, then $\langle\sigma\rangle \subseteq N_G(H)$. It follows that $\langle\sigma\rangle \times H$ has an element of order pk, $k > 1$, a contradiction. This implies that $N_G(H) = G_m$.

(vi). Since $\gcd(p, d) = 1$ and $\langle\sigma\rangle \lhd G$, we have $\langle\sigma\rangle H = \langle\sigma\rangle \rtimes H$. Since

$$H \cong (\langle\sigma\rangle \rtimes H)/\langle\sigma\rangle$$

where $(\langle\sigma\rangle \rtimes H)/\langle\sigma\rangle$ is isomorphic to a subgroup of $\langle\tau\rangle$, H is cyclic. This together with (iii) implies that $H \subseteq G_m$ for some m.

□

By Galois correspondence, we have the following description for the subfields of $K := \mathbb{Q}(x_1, \cdots, x_p)$ containing $F := K^{F_{p(p-1)}}$.

Theorem 2.2.6. *Let $K := \mathbb{Q}(x_1, \cdots, x_p)$, $F := K^{F_{p(p-1)}}$ and $k := \mathbb{Q}(s_1, \cdots, s_p)$.*

(i). F is a minimal subfield of K that contains k.

(ii). For each divisor d of $p-1$, there exists a unique subfield $E' := K^{\mathbb{Z}_p \rtimes \mathbb{Z}_{(p-1)/d}}$ of K containing F such that $[E' : F] = d$ which is normal over F. Furthermore, every normal extension E' of F contained in K is the fixed field of some normal subgroup containing G' with $[E' : F]|(p-1)$.

(iii). For each d dividing $p-1$, there exist p distinct subfields of K of degree pd over F and each of these subfields contains a unique fixed field K^{G_m} for some m. Moreover, for two subfields F_1 and F_2 which contains the same unique fixed field K^{G_m}, $F_1 \subseteq F_2$ if and only if $[F_1 : F]|[F_2 : F]$.

(iv). Any intermediate field of K and F arises from either (ii) or (iii).

We shall devote the rest of this section to introduce the Lagrange resolvents and other associated invariants. Our final objective is to provide the global view on the subfields of L that contains F.

Definition 2.2.7. *A Galois extension K/E is said to be abelian (respectively cyclic) if its Galois group G is abelian (respectively cyclic).*

Definition 2.2.8. *Let K/E be a cyclic extension over a field E of characteristic not dividing n which contains the nth roots of unity. Let σ be a generator for the cyclic group $Gal(K/E)$. For $\alpha \in K$ and any nth root of unity ζ, define the Lagrange resolvent $(\alpha, \zeta) \in K$ by*

$$(\alpha, \zeta) := \sum_{j=0}^{n-1} \zeta^j \sigma^j(\alpha)\,.$$

Definition 2.2.9. *For each $0 \leq j \leq p-1$, define $r_j := (x_1, \zeta^j)$ and $R_j := r_j^p$. Expanding r_1^p yields*

$$R_1 := r_1^p = (x_1, \zeta)^p = \sum_{j=0}^{p-1} l_j \zeta^j$$

where l_j is the sum of the terms in $(x_1, z)^p$ involving powers z^i with $i \equiv j \pmod{p}$.

Example 2.2.10. For the particular case when $p = 7$, we carry out an explicit calculation using Mathematica and saved this in a file named `lagres.nb`. We expand r_1^7 and collect terms with the same exponent for ζ. From this multinomial expansion, we express each l_j as a polynomial in the variables $x_1, \cdots, x_7$ and state this form for l_j in the appendix.

We quote the next result from [L] without proof.

Theorem 2.2.11. *Let $\alpha_1, \cdots, \alpha_n$ be distinct non-zero elements of a field K. If $a_1, \cdots, a_n$ are elements of K such that for all integers $v \geq 0$ we have*

$$a_1\alpha_1^v + \cdots + a_n\alpha_n^v = 0$$

then $a_i = 0$ for all i.

Corollary 2.2.12. *Let $\psi : \zeta \mapsto \zeta^s$ be the automorphism of L that acts trivially on $x_1, \cdots, x_p$. If $a_0, \cdots, a_{p-1}$ are elements of L such that*

(i).

$$a_0 + \cdots + a_{p-1} = 0\,,$$

(ii). $\psi(a_i) = a_i$ for all $0 \leq i \leq p-1$ and

(*iii*).

$$a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1} = 0\,,$$

then $a_i = 0$ *for each* $0 \leq i \leq p-1$.

Proof. We argue that

$$\sum_{j=0}^{p-1} a_j \zeta^{jv} = 0$$

for all integers $v \geq 0$. When v is a multiple of p,

$$\sum_{j=0}^{p-1} a_j \zeta^{jv} = \sum_{j=0}^{p-1} a_j = 0\,.$$

For $v \in \mathbb{Z}_p^*$, $v = s^n$ for some $1 \leq n \leq p-1$. Therefore

$$\sum_{j=0}^{p-1} a_j \zeta^{jv} = \sum_{j=0}^{p-1} a_j \psi^n(\zeta^j) = 0\,.$$

Invoking Theorem 2.2.11 then yields our desired conclusion. □

The next remark will prove to be useful in the succeeding lemma.

Remark 2.2.13. Taking $j = 0$ in Definition 2.2.9, we have $r_0 = s_1$ and

$$\sum_{j=0}^{p-1} l_j = s_1^p\,.$$

Consequently for any automorphism γ that acts trivially on

$$\sum_{j=0}^{p-1} l_j\,,$$

$\gamma(l_j) - l_j$ $(j = 0,\, 1,\, \cdots,\, p-1)$ satisfies hypothesis (i) of Corollary 2.2.12.

Adopting our definition of σ, τ and ψ as before, by direct calculation, the action of σ, τ and ψ on r_j, R_j and l_j is as follows:

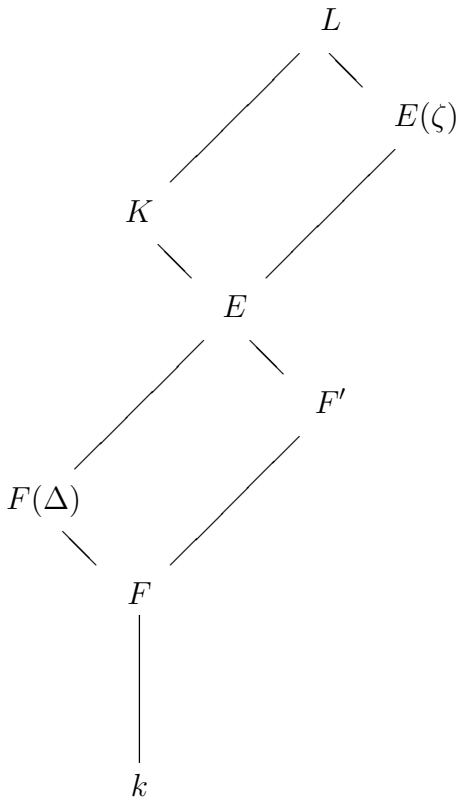
Lemma 2.2.14. *For* $0 \leq j \leq p-1$,

$$\sigma(r_j) = \zeta^{-j} r_j\,, \tau(r_j) = \psi^{-1}(r_j) = r_{s^{-1}j}$$

where s^{-1} *is the multiplicative inverse of* s *in* $\mathbb{Z}_p$. *Hence* $R_j \in E(\zeta)$, $l_j \in E$ *and* $\tau(l_j) = l_{sj}$ *for each* $0 \leq j \leq p-1$ *by Corollary* 2.2.12.

Applying Galois correspondence to Lemma 2.2.14 and Remark 2.2.3(ii) yields the following description of the fields K, k, F, E and L.

Theorem 2.2.15. *The lattice diagram for the fields K, k, F, $F(\Delta)$, E, F' and L is as follows:*



Moreover, $l_0 \in F$ and $l_1, \cdots, l_{p-1}$ are the roots of a polynomial $g(x)$ of degree $p-1$ over F and the field $E := F(l_1)$ is a cyclic extension of F of degree $p-1$ with $Gal(E/F) = \langle \tau|_E \rangle$. The unique quadratic subfield of E/F is the field $F(\Delta)$.

Notice that E being generated by l_1 over F shows that the other invariants l_j, $2 \leq j \leq p-1$ are F-linear combinations of 1, l_1, l_1^2, $\cdots$, l_1^{p-2} which in principle permits us to write down each of the R_j explicitly in radicals provided we can express a primitive pth root of unity in radicals.

To motivate the use of Lagrange resolvents, we shall quote the next result from [T] without proof.

Theorem 2.2.16. *Let $x_1, \cdots, x_n$ be roots of a irreducible polynomial of degree n over $\mathbb{Q}$. Then for $k = 1, \cdots, n$,*

$$x_k = \frac{1}{n} \sum_{j=0}^{n-1} \zeta^{j(1-k)} r_j \, .$$

2.3 Setting Up the Calculation

In the previous section, we have provided the necessary qualitative data one needs to solve the roots of a irreducible solvable polynomial $f(x)$ of degree p. Having done all these, we shall consider the main problem of doing the explicit calculation to express the roots in radicals and highlight the technicalities involved. Since the case for $p = 7$ still remains open and the case $p = 3$ is well known, we shall not be overly ambitious and just be concerned with the quintic case here and leave the septic case for performing explicit calculations to Section 3.1. Keeping these in mind, we shall break down the main problem into the following points of consideration:

(i). Finding the coefficients of the degree $p-1$ polynomial $g(x)$ with l_j, $1 \leq j \leq p-1$ as roots. This amounts to expressing the symmetric functions of the l_j in terms of the symmetric functions of the roots for $f(x)$.

(ii). Solving $g(x)$ (not necessarily irreducible) for l_j and labelling the roots obtained l'_j correctly.

(iii). Expressing a fixed primitive pth root of unity in terms of radicals.

(iv). Taking the appropriate pth root of each R_j formed to obtain r_j.

We begin with the following observation.

Remark 2.3.1. Since $Gal(E/F)$ is cyclic of order $p-1$, $l_1, \cdots, l_{p-1}$ are the roots of a polynomial of degree $p-1$ over F which factors over $F(\Delta)$ into the product of two conjugate polynomials of degree $(p-1)/2$:

$$\left[x^{(p-1)/2} + \sum_{m=0}^{(p-3)/2} (T_{2m+1} + T_{2m+2}\Delta)\, x^m \right] \left[x^{(p-1)/2} + \sum_{m=0}^{(p-3)/2} (T_{2m+1} - T_{2m+2}\Delta)\, x^m \right]$$

with $T_j \in F$ for all $1 \leq j \leq p-1$. We see that under the action of the subgroup $\langle \tau^2 \rangle$, the roots of one of these factors are the elements of the orbit containing l_1: $l_1, l_{s^2}, \cdots, l_{s^{p-3}}$ and the roots of the other factor are the elements of the orbit containing l_s: $l_s, l_{s^3}, \cdots, l_{s^{p-2}}$.

For the case when $p = 5$, instead of finding the coefficients of $g(x)$, Dummit (cf. [D]) factorized this quartic into the product of two conjugate quadratics over $F(\Delta)$ (see Remark 2.3.1) and computed the coefficients of these two quadratics. This is done by first writing each invariant in F as a linear combination of $1, \theta, \cdots, \theta^5$ over k where θ is a fixed invariant in F and applying the automorphisms generated by (1, 2, 3) and (1, 2) to generate complements of F_{20} in S_5. The coefficients of the resulting 6×6 system of linear equations are then solved using Cramer's rule.

Before we proceed to discuss step (ii), we need the following result which follows from Theorem 2.2.15.

Theorem 2.3.2. *Suppose $f(x)$ is a irreducible solvable polynomial of degree p and $g(x)$ is the degree $p-1$ polynomial with $l_1, \cdots, l_{p-1}$ as roots where l_j is defined as in Definition 2.2.9. Then the Galois group of $f(x)$ G is isomorphic to $\mathbb{Z}_p \rtimes \mathbb{Z}_d$ if and only if $g(x)$ factorizes into a product of $(p-1)/d$ irreducibles each of degree d over $\mathbb{Q}$.*

Proof. Since $[K : E] = p$, G is isomorphic $\mathbb{Z}_p \rtimes \mathbb{Z}_d$ if and only if $[E : \mathbb{Q}] = d$. Because

(i). $\langle \tau|_E \rangle$ being the Galois group of E over $\mathbb{Q}$ acts on the collection of generators $\{l_1, \cdots, l_{p-1}\}$ of E over F and

(ii). elements in the same orbit are conjugates of the same minimal polynomial,

$[E : \mathbb{Q}] = d$ is equivalent to the fact that $g(x)$ factorizes into a product of $(p-1)/d$ irreducibles each of degree d over $\mathbb{Q}$. □

In the case for quintics, Dummit's approach to calculate the coefficients of the two quadratic factors directly has several advantages as compared to computing the coefficients of $g(x)$. It facilitated greater ease in solving for the l_j and obtaining the factorization of $g(x)$ into irreducibles when $Gal(f(x)) \cong D_{10}$. In addition, since the roots of the quadratics give $\{l_1, l_4\}$ and $\{l_2, l_3\}$ up to a permutation of the 2 pairs, more information is known to identify the l_j correctly.

To label the l_j correctly for $p = 5$, a square root of the discriminant Δ' is fixed and assuming knowledge beforehand whether this corresponds to the Δ determined by the initial labelling of the roots x_j, the l'_j obtained are arranged so that

$$(l'_1 - l'_4)(l'_2 - l'_3) = \Theta\Delta' \text{ where } \Theta = \frac{(l_1 - l_4)(l_2 - l_3)}{\Delta} \in K\,.$$

This restriction narrows down to the 4 legitimate labelling of l'_1, l'_2, l'_3, l'_4 which are

$$l_1\,, l_2\,, l_3\,, l_4\,,$$
$$l_4\,, l_3\,, l_2\,, l_1\,,$$
$$l_2\,, l_4\,, l_1\,, l_3\,,$$
$$l_3\,, l_1\,, l_4\,, l_2\,.$$

We next characterize all the legitimate labelling of l_j for a fixed odd prime p.

Remark 2.3.3. Let $X := \{1\,, \cdots, p\}$ and $Y := \{l_j \,|\, 1 \leq j \leq p-1\}$.

(i). Suppose X is permuted by some $\gamma \in S_p$. For u, $v \in X$ such that $\gamma(u) = v$, the corresponding p-cycle that we have fixed in Remark 2.2.3 is $\sigma' : v \mapsto \gamma(u+1)$. Hence $\sigma' = (1,\ \gamma(\gamma^{-1}(1)+1),\ \cdots,\ \gamma(\gamma^{-1}(1)+p-1))$. For each $1 \leq j \leq p-1$, let r'_j denote the respective Lagrange resolvents, $R'_j := r'^p_j$ and l'_j be the sum of the terms in $(x'_1, z)^p$ involving powers z^i with $i \equiv j \pmod p$. By definition,

$$r'_j = \zeta^{j(1-\gamma^{-1}(1))} r_j\,.$$

Thus $R'_j = R_j$ and $l'_j = l_j$ for all $1 \leq j \leq p-1$.

(ii). Lemma 2.2.14 implies that for any $\gamma \in F_{p(p-1)}$, γ induces an automorphism of Y which coincides with the automorphism on Y induced by τ^n for some $1 \leq n \leq p-1$. In particular, this induced automorphism of Y is uniquely determined by its image on l_1 and any permutation of Y that arises this way must be one of the following:

$$id(Y) :\ l_1\,, \cdots, l_{p-1}\,,$$
$$\tau(Y) :\ l_s\,, \cdots, l_{-s}\,,$$
$$\cdots\,, \cdots\,, \cdots\,, \cdots\,, \cdots\,,$$
$$\tau^{p-2}(Y) :\ l_{s^{p-2}}\,, \cdots, l_{-s^{p-2}}\,.$$

Remark 2.3.3(ii) says that we may choose any of the l_j to be l'_1 and the rest of the l'_j is uniquely determined by this choice theoretically. From the computational point of view, this does not seem to be efficient as there will be $(p-2)!$ ways to permute $Y - \{l'_1\}$. In practice, after obtaining the radical expression of each l'_j by solving $g(x)$, we approximate the roots of $f(x)$ to sufficiently high precision and fix a permutation of X. The l'_j are then computed

numerically using their formal definition and compared to the numerical values of each radical expression of l'_j to ensure that the radical expressions of each l'_j are labelled correctly.

We begin our discussion of (iii) by stating the next result from [L] without proof.

Theorem 2.3.4. *Let ω be a primitive nth root of unity and σ denote the automorphism of $\mathbb{Q}(\omega)$ over $\mathbb{Q}$ such that $\sigma(\omega) = \omega^j$. The map $\sigma \mapsto j$ gives an isomorphism*

$$Gal(\mathbb{Q}(\omega)/\mathbb{Q}) \longrightarrow \mathbb{Z}_n^* .$$

In particular,

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$$

where φ denotes the Euler-phi function.

For our purpose, we restrict our attention to the case when n is an odd prime p and let $\omega := e^{2\pi i/p}$.

Remark 2.3.5. Let s be a primitive root of $\mathbb{Z}_p$. It follows from Theorem 2.3.4 that the map $\Psi : \omega \mapsto \omega^s$ is a generator of $Gal(\mathbb{Q}(\omega)/\mathbb{Q})$. Therefore for every divisor of $p-1$, $\langle \Psi^{(p-1)/d} \rangle$ is the unique subgroup of order d. Furthermore, given any two divisors d and d' of $p-1$, $\langle \Psi^{(p-1)/d} \rangle \subseteq \langle \Psi^{(p-1)/d'} \rangle$ if and only if $d|d'$. Translating this information on the subgroups of $Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ to the corresponding fixed fields by Galois correspondence, for every divisor d of $p-1$, there exists a unique subfield of $\mathbb{Q}(\omega)$ of degree d over $\mathbb{Q}$ that corresponds to the subgroup $\langle \Psi^d \rangle$. In addition, for two such subfields E and F of degree d and d' over $\mathbb{Q}$ respectively, $E \supseteq F$ if and only if $d'|d$. When this is the case, E/F is Galois with $Gal(E/F) \cong \langle \Psi^{d'} \rangle / \langle \Psi^d \rangle$.

Proposition 2.3.6. *(i). $\mathbb{Q}(\cos \frac{2\pi}{p})$ is the unique subfield of $\mathbb{Q}(\omega)$ of degree $(p-1)/2$ over $\mathbb{Q}$. In addition, $\mathbb{Q}(\cos \frac{2\pi}{p})/\mathbb{Q}$ is Galois with*

$$Gal(\mathbb{Q}(\cos \tfrac{2\pi}{p})/\mathbb{Q}) \cong \langle \Psi \rangle / \langle \Psi^{(p-1)/2} \rangle .$$

(ii). The elements of $S := \{ \omega^j + \omega^{-j} \mid 1 \leq j \leq (p-1)/2 \}$ are precisely all the conjugates of $\omega + \omega^{-1}$ over $\mathbb{Q}$.

Proof. (i).

$$\cos \tfrac{2\pi}{p} = \tfrac{1}{2}(\omega + \omega^{-1})$$

remains invariant under a non identity automorphism $\sigma \in Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ if and only if $\sigma(\omega) = \omega^{-1}$, i.e. σ is an involution. (i) then follows by Remark 2.3.5.

(ii). By Artin's theorem, it suffices to show that $S := \{\, \Psi^j(\omega+\omega^{-1}) \,|\, 1 \leq j \leq (p-1)/2 \,\}$. Since the automorphisms $\Psi^j/\langle\Psi^{(p-1)/2}\rangle$ are all distinct for $1 \leq j \leq (p-1)/2$, it follows that $(\Psi(\omega+\omega^{-1}), \cdots, \Psi^{(p-1)/2}(\omega+\omega^{-1}))$ are all distinct and thus differs from $(\omega+\omega^{-1}, \cdots, \omega^{(p-1)/2}+\omega^{(1-p)/2})$ by a permutation.

□

Since it is easy to solve the quadratic equation $x^2 - (\omega+\omega^{-1})x + 1 = 0$ for ω, the problem of solving ω reduces to solving the minimal polynomial of $\omega+\omega^{-1}$ which is of degree $\frac{p-1}{2}$ over $\mathbb{Q}$ and can be computed from the pth cyclotomic polynomial $x^{p-1}+\cdots+1$ by performing the substitution $y = x+\frac{1}{x}$.

Example 2.3.7. Applying the technique outlined above to calculate $e^{2\pi i/5}$, we obtain

$$2\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{2}\,, 2\cos\frac{4\pi}{5} = \frac{-1-\sqrt{5}}{2}\,.$$

It remains to consider the choice of the pth roots of the R_j to obtain the Lagrange resolvents r_j. Before we state and prove the next result which asserts that, given $R_1 = r_1^p$, each of the p possible choices for r_1 uniquely determines r_j as a pth root of R_j $(2 \leq j \leq p-1)$, we shall need to make the following observations.

Remark 2.3.8. Viewing $x_1, \cdots, x_p$ as the roots of $f(x)$, recall that K is defined as the splitting field of $f(x)$, $k := \mathbb{Q}$, $E := K^{\langle\sigma\rangle}$, $L := K(\zeta)$ and s is a fixed primitive generator of $\mathbb{Z}_p^*$.

(i). We deduce that the automorphism $\psi : \zeta \mapsto \zeta^s$ that acts trivially on $x_1, \cdots, x_p$ exists by natural irrationalities since the restriction of each automorphism in $Gal(L/K)$ to $k(\zeta)$ gives an isomorphism of $Gal(L/K)$ onto the Galois group of $k(\zeta)$ over $k(\zeta) \cap K$.

(ii). $r_j \notin \mathbb{Q}$ for all $1 \leq j \leq p-1$. In particular, r_j is non-vanishing for each $1 \leq j \leq p-1$. Suppose otherwise $r_j \in \mathbb{Q}$ for some $1 \leq j \leq p-1$. Applying ψ iteratively $p-2$ times, we see that $r_j = r_1$ for all $2 \leq j \leq p-1$. It follows from Theorem 2.2.16 and Remark 2.2.13 that

$$x_1 = \frac{1}{p}\sum_{j=0}^{p-1} r_j = \frac{1}{p}\Big[s_1 + (p-1)r_1\Big] \in \mathbb{Q}\,.$$

This contradicts the fact that $[\mathbb{Q}(x_1) : \mathbb{Q}] = p > 1$.

We now state and prove the result formally.

Theorem 2.3.9. *Given r_1, for each $2 \leq j \leq p-1$, there is a unique choice of r_j such that the equation $R_j := r_j^p$ is satisfied.*

Proof. Since

(i). the action of ψ on $\{r_1, \cdots, r_{p-1}\}$ is transitive and

(ii). $r_j \neq 0$ for all $2 \leq j \leq 6$ by Remark 2.3.8(ii),

the theorem follows. □

For the sake of performing explicit calculations, we derive the following proposition which follows from Lemma 2.2.14.

Proposition 2.3.10. *Let $d > 1$ be a divisor of $p-1$ and $d' = \frac{p-1}{d}$. For $1 \leq j \leq p-1$,*

$$\prod_{n=1}^{d} r_{js^{nd'}}$$

is fixed by σ, $\tau^{d'}$ and $\tau^{d'-1}\psi^{-1}$ and so is in the fixed field of $\langle \sigma\,, \tau^{d'}\,, \tau^{d'-1}\psi^{-1} \rangle$ in L which is of degree d' over F. In particular,

(i).

$$\prod_{n=1}^{2} r_{js^{n(p-1)/2}}$$

is fixed by σ, $\tau^{(p-1)/2/}$ and $\tau^{(p-3)/2}\psi^{-1}$.

(ii).

$$\prod_{n=1}^{(p-1)/2} r_{js^{2n}}$$

is fixed by σ, τ^2 and $\tau\psi^{-1}$ and hence lies in $F\left(\Delta\sqrt{(-1)^{(p-1)/2}p}\right)$.

Using Proposition 2.3.10, Dummit created the following invariants

$$r_1r_4\,, r_2r_3\,, r_1r_2^2 + r_4r_3^2\,, r_3r_1^2 + r_2r_4^2 \in F(\Delta\sqrt{5})$$

and used them to determine uniqueness for r_2, r_3 and r_4. For completeness, we shall state this result without proof here and refer the interested reader to [D] for the the proof.

Theorem 2.3.11. *Given r_1, there is a unique choice of r_2, r_3, r_4 such that*

$$r_1r_4\,, r_2r_3\,, r_1r_2^2 + r_4r_3^2\,, r_3r_1^2 + r_2r_4^2$$

are fixed invariants of $F(\Delta\sqrt{5})$.

Chapter 3

Solvable Septics

After giving a brief survey for the general case when p is an odd prime, we shall now focus on the case for $p = 7$. We will also devote this chapter to giving an explicit example that exhibits calculations in solving solvable polynomials of degree 7 with Galois group isomorphic to $\mathbb{Z}_7$ by applying the core results in Chapter 2.

Throughout this chapter, we let $\zeta := e^{2\pi i/7}$, x_1, x_2, x_3, x_4, x_5, x_6, x_7 denote the roots of the general septic polynomial

$$f(x) := x_7 - s_1x^6 + s_2x^5 - s_3x^4 + s_4x^3 - s_5x^2 + s_6x - s_7$$

where the s_j are the symmetric functions in the roots as defined in Definition 2.2.1. For simplicity, we let $\sqrt[n]{\ }$ denote the principal nth root, i.e. for $z = re^{i\theta} \neq 0$ where $\theta \in (-\pi, \pi]$ is the principal argument of z,

$$\sqrt[n]{z} = r^{1/n}e^{\theta i/n}\,.$$

3.1 Lagrange Resolvents for Septic Polynomials

Throughout this section, we adopt Definition 2.2.9 to state the following Lagrange resolvents:

$$r_0 := (x_1, 1) := x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 = s_1\,,$$

$$r_1 := (x_1, \zeta) := x_1 + x_2\zeta + x_3\zeta^2 + x_4\zeta^3 + x_5\zeta^4 + x_6\zeta^5 + x_7\zeta^6\,,$$
$$r_2 := (x_1, \zeta^2) := x_1 + x_2\zeta^2 + x_3\zeta^4 + x_4\zeta^6 + x_5\zeta + x_6\zeta^3 + x_7\zeta^5\,,$$

$$r_3 := (x_1, \zeta^3) := x_1 + x_2\zeta^3 + x_3\zeta^6 + x_4\zeta^2 + x_5\zeta^5 + x_6\zeta + x_7\zeta^4\,,$$
$$r_4 := (x_1, \zeta^4) := x_1 + x_2\zeta^4 + x_3\zeta + x_4\zeta^5 + x_5\zeta^2 + x_6\zeta^6 + x_7\zeta^3\,,$$
$$r_5 := (x_1, \zeta^5) := x_1 + x_2\zeta^5 + x_3\zeta^3 + x_4\zeta + x_5\zeta^6 + x_6\zeta^4 + x_7\zeta^2\,,$$
$$r_6 := (x_1, \zeta^6) := x_1 + x_2\zeta^6 + x_3\zeta^5 + x_4\zeta^4 + x_5\zeta^3 + x_6\zeta^2 + x_7\zeta\,.$$

It follows from Theorem 2.2.16 that

$$x_1 = (r_0 + r_1 + r_2 + r_3 + r_4 + r_5 + r_6)/7\,,$$

$$x_2 = (r_0 + \zeta^6 r_1 + \zeta^5 r_2 + \zeta^4 r_3 + \zeta^3 r_4 + \zeta^2 r_5 + \zeta r_6)/7\,,$$
$$x_3 = (r_0 + \zeta^5 r_1 + \zeta^3 r_2 + \zeta r_3 + \zeta^6 r_4 + \zeta^4 r_5 + \zeta^2 r_6)/7\,,$$
$$x_4 = (r_0 + \zeta^4 r_1 + \zeta r_2 + \zeta^5 r_3 + \zeta^2 r_4 + \zeta^6 r_5 + \zeta^3 r_6)/7\,,$$
$$x_5 = (r_0 + \zeta^3 r_1 + \zeta^6 r_2 + \zeta^2 r_3 + \zeta^5 r_4 + \zeta r_5 + \zeta^4 r_6)/7\,,$$
$$x_6 = (r_0 + \zeta^2 r_1 + \zeta^4 r_2 + \zeta^6 r_3 + \zeta r_4 + \zeta^3 r_5 + \zeta^5 r_6)/7\,,$$
$$x_7 = (r_0 + \zeta r_1 + \zeta^2 r_2 + \zeta^3 r_3 + \zeta^4 r_4 + \zeta^5 r_5 + \zeta^6 r_6)/7\,.$$

Similarly, we have

$$R_1 := r_1^7 = l_0 + l_1\zeta + l_2\zeta^2 + l_3\zeta^3 + l_4\zeta^4 + l_5\zeta^5 + l_6\zeta^6\,,$$

$$R_2 := r_2^7 = l_0 + l_4\zeta + l_1\zeta^2 + l_5\zeta^3 + l_2\zeta^4 + l_6\zeta^5 + l_3\zeta^6\,,$$
$$R_3 := r_3^7 = l_0 + l_5\zeta + l_3\zeta^2 + l_1\zeta^3 + l_6\zeta^4 + l_4\zeta^5 + l_2\zeta^6\,,$$
$$R_4 := r_4^7 = l_0 + l_2\zeta + l_4\zeta^2 + l_6\zeta^3 + l_1\zeta^4 + l_3\zeta^5 + l_5\zeta^6\,,$$
$$R_5 := r_5^7 = l_0 + l_3\zeta + l_6\zeta^2 + l_2\zeta^3 + l_5\zeta^4 + l_1\zeta^5 + l_4\zeta^6\,,$$
$$R_6 := r_6^7 = l_0 + l_6\zeta + l_5\zeta^2 + l_4\zeta^3 + l_3\zeta^4 + l_2\zeta^5 + l_1\zeta^6\,.$$

When $f(x)$ is solvable, its Galois group is a transitive subgroup of F_{42} by Corollary 2.1.7. Adopting the same notations as in Remark 2.2.3, we fix 3 as our choice for s, a fixed primitive root of $\mathbb{Z}_7$ and set $\sigma := (1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7)$, $\tau := (2,\ 4,\ 3,\ 7,\ 5,\ 6)$ acting trivially on ζ and $\psi : \zeta \mapsto \zeta^3$ acting trivially on $x_1, \cdots, x_7$.

By Lemma 2.2.14, the action of σ, τ and ψ on r_j and l_j $(1 \le j \le 6)$ is as follows:

$$\sigma(r_1) = \zeta^6 r_1,\ \tau(r_1) = \psi^5(r_1) = r_5,$$
$$\sigma(r_2) = \zeta^5 r_2,\ \tau(r_2) = \psi^5(r_2) = r_3,$$
$$\sigma(r_3) = \zeta^4 r_3,\ \tau(r_3) = \psi^5(r_3) = r_1,$$

$$\sigma(r_4) = \zeta^3 r_4,\ \tau(r_4) = \psi^5(r_4) = r_6,$$
$$\sigma(r_5) = \zeta^2 r_5,\ \tau(r_5) = \psi^5(r_5) = r_4,$$
$$\sigma(r_6) = \zeta r_6,\ \tau(r_6) = \psi^5(r_6) = r_2\,.$$

We shall now review the four problems that were proposed in the previous section for $p = 7$.

In solving quintics, recall that Dummit first calculate those elements in the fixed field of the Frobenius group by generating complements of F_{20} in S_5 and solving a 6×6 system of linear equations. The equivalent computation for the case $p = 7$ would not be computationally feasible as it requires us to solve a 120×120 system of linear equations. For the case of sextic polynomials, it was cited in [H] that the evaluation of a determinant for a 15×15 matrix symbolically is still not known.

Theorem 3.1.1. *Suppose $f(x)$ is a irreducible solvable septic and $g(x)$ is the degree 6 polynomial with $l_1, \cdots, l_6$ as roots where l_j is defined as in Definition 2.2.9. Then the Galois group of $f(x)$ is $\mathbb{Z}_7 \rtimes \mathbb{Z}_d$ if and only if $g(x)$ factorizes into a product of $6/d$ irreducibles each of degree d over $\mathbb{Q}$.*

Recall from Corollary 2.1.7 that a solvable septic $f(x)$ can only have Galois group isomorphic to either $\mathbb{Z}_7$, D_{14}, $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$ or F_{42}. When $Gal(f(x)) \cong \mathbb{Z}_7$, we multiply $g(x)$ by a suitable positive positive rational so that the resulting polynomial $h(x)$ have coprime integral coefficients. Since all l_j are rational with numerator and denominator dividing the constant term and leading term of $h(x)$ respectively, an exhaustive search can be implemented on the computer to solve for the l_j. When $Gal(f(x)) \cong F_{42}$, $g(x)$ is irreducible of degree 6 with Galois group isomorphic to $\mathbb{Z}_6$. Hence we may appeal to the results in [H] to obtain the l_j. When $Gal(f(x)) \cong D_{14}$, we know that $g(x)$ factorizes into 3 irreducible quadratics over $\mathbb{Q}$ by Theorem 3.1.1 but to obtain this factorization explicitly is non-trivial in general. The case for solving l_j from $g(x)$ when $Gal(f(x)) \cong \mathbb{Z}_7 \rtimes \mathbb{Z}_3$ faces a similar technicality.

It is not clear how we can design an algorithm to label the l_j correctly for $p = 7$.

We now restate the analogous statements in Remark 2.3.3(ii).

Remark 3.1.2. For any $\gamma \in F_{42}$, γ induces an automorphism of Y which coincides with the automorphism on Y induced by τ^n for some $1 \le n \le 6$. In particular, this induced automorphism of Y is uniquely determined by its image on l_1 and any permutation of Y that arises this way must be one of the following:

$$id(Y) :\ l_1\,, l_2\,, l_3\,, l_4\,, l_5\,, l_6\,,$$

$$\begin{aligned}
\tau(Y) &: l_3,\, l_6,\, l_2,\, l_5,\, l_1,\, l_4\,,\\
\tau^2(Y) &: l_2,\, l_4,\, l_6,\, l_1,\, l_3,\, l_5\,,\\
\tau^3(Y) &: l_6,\, l_5,\, l_4,\, l_3,\, l_2,\, l_1\,,\\
\tau^4(Y) &: l_4,\, l_1,\, l_5,\, l_2,\, l_6,\, l_3\,,\\
\tau^5(Y) &: l_5,\, l_3,\, l_1,\, l_6,\, l_4,\, l_2\,.
\end{aligned}$$

We adopt the method mentioned in Section 2.3 to perform the following calculation which expresses the non-trivial 7th roots of unity in radicals.

Example 3.1.3. By making the substitution $y := x + \frac{1}{x}$ to

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0\,,$$

we see that $\zeta + \zeta^{-1}$ is a root of

$$y^3 + y^2 - 2y - 1 \;=\; 0\,. \tag{3.1.1}$$

Using Proposition 2.3.6, we deduce that $y^3 + y^2 - 2y - 1$ is the minimal polynomial of $\zeta+\zeta^{-1}$ and its roots are precisely $2\cos\frac{2\pi}{7} = \zeta+\zeta^{-1}$, $2\cos\frac{4\pi}{7} = \zeta^2 + \zeta^{-2}$ and $2\cos\frac{6\pi}{7} = \zeta^3 + \zeta^{-3}$. Since $\cos\frac{6\pi}{7} < \cos\frac{4\pi}{7} < \cos\frac{2\pi}{7}$, solving equation (3.1.1) by direct calculation using Cardan's formula, we conclude that

$$\cos\frac{2\pi}{7} = \frac{1}{6}\left[-1 + \sqrt[3]{\frac{98}{1+3\sqrt{3}i}} + \sqrt[3]{\frac{7}{2}\left(1+3\sqrt{3}i\right)}\right]\,,$$

$$\cos\frac{4\pi}{7} = -\frac{1}{12}\left[2 + (1-\sqrt{3}i)\sqrt[3]{\frac{98}{1+3\sqrt{3}i}} + (1+\sqrt{3}i)\sqrt[3]{\frac{7}{2}\left(1+3\sqrt{3}i\right)}\right]\,,$$

$$\cos\frac{6\pi}{7} = -\frac{1}{12}\left[2 + (1+\sqrt{3}i)\sqrt[3]{\frac{98}{1+3\sqrt{3}i}} + (1-\sqrt{3}i)\sqrt[3]{\frac{7}{2}\left(1+3\sqrt{3}i\right)}\right]\,.$$

Implementing the relation $\sin\theta = \sqrt{1-\cos^2\theta}$ for $0 \le \theta \le \pi$, we have

$$\sin\frac{2\pi}{7} = \frac{1}{2u}\sqrt{\frac{1}{3}\sqrt[3]{\frac{7}{4}}\left[2v + (1-\sqrt{3}i)w + 2\sqrt[3]{2}(-2+\sqrt{3}i)\right]}\,,$$

$$\sin\frac{4\pi}{7} = \frac{1}{2u}\sqrt{\frac{1}{3}\sqrt[3]{\frac{7}{4}}\left[2v + (1+\sqrt{3}i)w + \sqrt[3]{2}(5+\sqrt{3}i)\right]}\,,$$

$$\sin\frac{6\pi}{7} = \frac{1}{2u}\sqrt{\frac{1}{3}\sqrt[3]{\frac{7}{4}}\left[2v - 2w - \sqrt[3]{2}(1+3\sqrt{3}i)\right]}\,,$$

where

$$u := \sqrt[3]{1+3\sqrt{3}i}\,,\ v := \sqrt[3]{49(-13+3\sqrt{3}i)}\,,\ w := \sqrt[3]{7(1+3\sqrt{3}i)}\,.$$

Since we are unable to express fixed invariants in terms of the symmetric functions of the roots explicitly in general to show uniqueness of r_j ($2 \leq j \leq 6$ given r_1, we shall only restate Theorem 2.3.9 for the septic case here.

Theorem 3.1.4. *Given r_1, for each $2 \leq j \leq 6$, there is a unique choice of r_j such that the equation $R_j := r_j^p$ is satisfied.*

3.2 Expressing $\cos\frac{2\pi}{29}$ in radicals

It is well known that for each natural number n, $\cos\frac{2\pi}{n}$ is algebraic. Moreover, in the quest of determining which n-sided regular polygon is constructible by straightedge and compass, Gauss showed how to express $\cos\frac{2\pi}{17}$ in radicals. The main purpose of this section is to perform an analogous calculation to express $\cos\frac{2\pi}{29}$ in radicals.

Throughout this section, all technical calculations performed using Mathematica are saved in a file named `lagres.nb`. Due to the overwhelming length of the output, we shall only present the commands of this program in the appendix.

Before we formally embark on the task of expressing $\cos\frac{2\pi}{29}$ in radicals, we investigate the possibility of expressing $\cos\frac{2\pi}{29}$ completely in real radicals.

Definition 3.2.1. *Define $\alpha \in \mathbb{R}$ to be a real radical element if it lies in some repeated radical extension of $\mathbb{Q}$ that is contained in $\mathbb{R}$.*

The following result is taken from [I]. For the convenience of the readers, the proof is included in the appendix.

Theorem 3.2.2. *Suppose $f(x) \in \mathbb{Q}[x]$ is an irreducible polynomial which splits over $\mathbb{R}$. If $f(x)$ has any root which is a real radical element, then the degree of $f(x)$ is a power of 2 and the Galois group of $f(x)$ over $\mathbb{Q}$ is a 2-group.*

Proposition 3.2.3. *$\cos\frac{2\pi}{p}$ is a real radical element if and only if p is a Fermat prime.*

Proof. Necessity follows at once, for if $p = 2^{2^m}+1$ for some $m \geq 0$, $\mathbb{Q}(\cos\frac{2\pi}{p}) \subseteq \mathbb{R}$ can be obtained at the end of a finite tower where each step of the tower is a radical extension of degree 2. To show sufficiency, since the minimal

polynomial of $\cos\frac{2\pi}{p}$ is of degree $(p-1)/2$ and splits over $\mathbb{R}$ by Proposition 2.3.6, we invoke Theorem 3.2.2 and see that $(p-1)/2 = 2^n$ for some $n \geq 0$. p being prime then forces n to be a power of 2. $\square$

It follows from Proposition 3.2.3 that $\cos\frac{2\pi}{29}$ cannot be completely expressed in real radicals.

Remark 3.2.4. We consider the case when $p = 29$. Since 2 is a primitive root of $\mathbb{Z}_{29}$, we may fix the automorphism $\Psi : \omega \mapsto \omega^2$. By Proposition 2.3.6 and Remark 2.3.5, $\mathbb{Q}(\cos\frac{2\pi}{29})$ is of degree 14 over $\mathbb{Q}$ and contains a unique subfield K of degree 7 over $\mathbb{Q}$. In view of this, $\cos\frac{2\pi}{29}$ satisfies a monic quadratic polynomial $h(x) \in K[x]$ as a root. To determine $h(x)$ explicitly, we apply the non identity automorphism $\Psi^7/\langle\Psi^{14}\rangle$ of $Gal(\mathbb{Q}(\cos\frac{2\pi}{29})/K)$ and see that the non trivial conjugate of $\omega + \omega^{28}$ over K is $\omega^{12} + \omega^{17}$. Hence

$$h(x) = x^2 - (\omega + \omega^{12} + \omega^{28} + \omega^{17})x + (\omega^{16} + \omega^{18} + \omega^{13} + \omega^{11})\,.$$

With this conclusion, we are able to express $\cos\frac{2\pi}{29}$ in radicals if we can do the same to $\omega + \omega^{12} + \omega^{28} + \omega^{17}$ and $\omega^{16} + \omega^{18} + \omega^{13} + \omega^{11}$. Applying the generator $\Psi/\langle\Psi^7\rangle$ of $Gal(K/\mathbb{Q})$ to $\omega + \omega^{12} + \omega^{28} + \omega^{17}$ cyclically and using Maple, we see that

$$\begin{aligned}
x_1 &:= \omega + \omega^{12} + \omega^{28} + \omega^{17}\,,\\
x_2 &:= \omega^2 + \omega^{24} + \omega^{27} + \omega^{5}\,,\\
x_3 &:= \omega^4 + \omega^{19} + \omega^{25} + \omega^{10}\,,\\
x_4 &:= \omega^8 + \omega^{9} + \omega^{21} + \omega^{20}\,,\\
x_5 &:= \omega^{16} + \omega^{18} + \omega^{13} + \omega^{11}\,,\\
x_6 &:= \omega^3 + \omega^{7} + \omega^{26} + \omega^{22}\,,\\
x_7 &:= \omega^6 + \omega^{14} + \omega^{23} + \omega^{15}\,,
\end{aligned}$$

are the roots of the septic polynomial $x^7+x^6-12x^5-7x^4+28x^3+14x^2-9x+1$.

Recall our definition for r_j and R_j for $0 \leq j \leq 6$. Motivated by Theorem 2.2.16, we shall proceed as follows.

Example 3.2.5. We substitute the actual values of $x_1, \cdots, x_7$ into the polynomial expression obtained for each l_j in Example 2.2.10. The values for l_3, l_2, l_6, l_4, l_5 are verified in this order by applying $\tau := (2,\ 4,\ 3,\ 7,\ 5,\ 6)$ repeatedly to $x_1, \cdots, x_7$. Our computation yields $l_0 = -45410$,

$$l_1 = -37058\,,\ l_2 = -46396\,,\ l_3 = 63224\,,$$

$$l_4 = 33383\,,\ l_5 = -26096\,,\ l_6 = 58352\ .$$

Consequently,

$$R_1 = 8352\zeta - 986\zeta^2 + 108634\zeta^3 + 78793\zeta^4 + 19314\zeta^5 + 103762\zeta^6\,,$$

$$R_2 = 78793\zeta + 8352\zeta^2 + 19314\zeta^3 - 986\zeta^4 + 103762\zeta^5 + 108634\zeta^6\,,$$

$$R_3 = 19314\zeta + 108634\zeta^2 + 8352\zeta^3 + 103762\zeta^4 + 78793\zeta^5 - 986\zeta^6\,,$$

$$R_4 = -986\zeta + 78793\zeta^2 + 103762\zeta^3 + 8352\zeta^4 + 108634\zeta^5 + 19314\zeta^6\,,$$

$$R_5 = 108634\zeta + 103762\zeta^2 - 986\zeta^3 + 19314\zeta^4 + 8352\zeta^5 + 78793\zeta^6\,,$$

$$R_6 = 103762\zeta + 19314\zeta^2 + 78793\zeta^3 + 108634\zeta^4 - 986\zeta^5 + 8352\zeta^6\,.$$

For each $1 \leq j \leq 6$, the ratio of r_j to $\sqrt[7]{R_j}$ is an integral power of ζ which we will denote by n_j. Hence

$$r_j \;=\; \zeta^{n_j}\sqrt[7]{R_j} \tag{3.2.1}$$

where n_j is some element of $\mathbb{Z}_7$. Since the principal argument of a product differs from the sum of the principal arguments of the factors by an integral multiple of 2π, we have

$$\frac{7\operatorname{Arg} r_j - \operatorname{Arg} R_j}{2\pi} \;\equiv\; n_j \pmod 7\,. \tag{3.2.2}$$

Evaluating the left hand side of equation (3.2.2) numerically to 400 decimal places using a for loop with index $1 \leq j \leq 6$ incrementing by one unit with each iteration yields an approximation for each n_j having absolute error less than 5×10^{401}. Therefore we can deduce

$$n_1 = 1,\, n_2 = 3,\, n_3 = 1,\, n_4 = 6,\, n_5 = 4,\, n_6 = 6\,.$$

Thus, assigning the variables a, b, c, d, e and f with the expression of ζ, ζ^2, ζ^3, ζ^4, ζ^5 and ζ^6 in radicals respectively, for $1 \leq j \leq 6$, we obtain each R_j and r_j in radicals. Finally, appealing to the relations

$$x_1 = \frac{1}{7}\sum_{j=0}^{6} r_j,\; x_5 = \frac{1}{7}\sum_{j=0}^{6} \zeta^{3j} r_j$$

from Theorem 2.2.16 and applying the formula

$$\cos\frac{2\pi}{29} = \frac{1}{4}\left(-x_1 + \sqrt{x_1^2 - 4x_5}\right)$$

yields what we sought out to compute initially. The interested reader is referred to the program `lagres.nb` in the appendix for the actual radical expression of R_j, r_j $(1 \leq j \leq 6)$, x_1 and x_5. Explicitly,

$$\begin{aligned} x_1 \;=\; & \tfrac{1}{504a_1}\big(-72a_1 + 2a_2a_3a_4a_{31} - 2a_{24}a_3a_1a_{31} + 2a_{29}a_3a_{15}a_1^2a_{31} \\ & -6ia_{30}a_{32}a_1a_{37}a_{31} + 2a_2a_3a_4a_{38} - 2a_{24}a_3a_1a_{38} + 2a_{29}a_3a_{15}a_1^2a_{38} \\ & +6ia_{30}a_{32}a_1a_{37}a_{38} - 6ia_{34}a_{32}a_4a_{43} - 2a_{34}a_3a_4a_{43} - 2a_{41}a_3a_1a_{43} \\ & +3ia_{42}a_{44}a_{15}a_1^2a_{43} - a_{42}a_3a_{15}a_1^2a_{43} + 6ia_{45}a_{44}a_1a_{48}a_{43} + 2a_2a_3a_4a_{52} \\ & -2a_{24}a_3a_1a_{52} + 2a_{29}a_3a_{15}a_1^2a_{52} + 6ia_{30}a_{44}a_1a_{37}a_{52} + 2a_2a_3a_4a_{58} \\ & -2a_{24}a_3a_1a_{58} + 2a_{29}a_3a_{15}a_1^2a_{58} - 6ia_{30}a_{32}a_1a_{37} - 6ia_{34}a_{32}a_4a_{59} \\ & -2a_{34}a_3a_4a_{59} - 2a_{41}a_3a_1a_{59} + 3ia_{42}a_{32}a_{15}a_1^2a_{59} - a_{42}a_3a_{15}a_1^2a_{59} \\ & -6ia_{45}a_{32}a_1a_{48}a_{59}\big) \end{aligned}$$

and

$$\begin{aligned}
x_5 \;=\; & \tfrac{1}{1008a_1^2}\big(-a_{57}a_1^2 - 18ia_{29}a_{44}a_{15}a_{31} - 2a_{29}a_3a_{15}a_{31} - 2a_2a_3a_4a_1a_{31} \\
& -4a_{24}a_3a_1^2a_{31} - ia_{60}a_{32}a_{15}a_{48}a_{31} + 3a_{60}a_3a_{15}a_{48}a_{31} \\
& -2ia_{61}a_{32}a_4a_1a_{48}a_{31} + 2ia_{30}a_{32}a_1^2a_{48}a_{31} + 5ia_{60}a_{44}a_{15}a_{37}a_{31} \\
& -a_{60}a_3a_{15}a_{37}a_{31} + ia_{61}a_{32}a_4a_1a_{37}a_{31} - a_{61}a_3a_4a_1a_{37}a_{31} \\
& +2ia_{30}a_{32}a_1^2a_{37}a_{31} - a_{24}a_3a_1^2a_{68}a_{31} - 18ia_{29}a_{32}a_{15}a_{38} - 2a_{29}a_3a_{15}a_{38} \\
& -2a_2a_3a_4a_1a_{38} - 4a_{24}a_3a_1^2a_{38} + ia_{60}a_{44}a_{15}a_{48}a_{38} - 3a_{60}a_3a_{15}a_{48}a_{38} \\
& +2ia_{61}a_{32}a_4a_1a_{48}a_{38} - 2ia_{30}a_{32}a_1^2a_{48}a_{38} - 5ia_{60}a_{32}a_{15}a_{37}a_{38} \\
& +a_{60}a_3a_{15}a_{37}a_{38} - ia_{61}a_{44}a_4a_1a_{37}a_{38} + a_{61}a_3a_4a_1a_{37}a_{38} \\
& -2ia_{30}a_{32}a_1^2a_{37}a_{38} - a_{24}a_3a_1^2a_{68}a_{38} - 18ia_{42}a_{44}a_{15}a_{43} - 2a_{42}a_3a_{15}a_{43} \\
& -4a_{34}a_3a_4a_1a_{43} - 4a_{41}a_3a_1^2a_{43} + ia_{67}a_{32}a_{15}a_{48}a_{43} - 3a_{67}a_3a_{15}a_{48}a_{43} \\
& +2ia_{70}a_{44}a_4a_1a_{48}a_{43} - 2ia_{45}a_{44}a_1^2a_{48}a_{43} + 5ia_{67}a_{44}a_{15}a_{37}a_{43} \\
& -a_{67}a_3a_{15}a_{37}a_{43} + ia_{70}a_{44}a_4a_1a_{37}a_{43} - a_{70}a_3a_4a_1a_{37}a_{43} \\
& +2ia_{45}a_{32}a_1^2a_{37}a_{43} + a_{41}a_3a_1^2a_{68}a_{43} + 12ia_{29}a_{44}a_{15}a_{52} - 8a_{29}a_3a_{15}a_{52} \\
& -3ia_2a_{32}a_4a_1a_{52} + a_2a_3a_4a_1a_{52} - 4a_{24}a_3a_1^2a_{52} + ia_{60}a_{44}a_{15}a_{69}a_{52} \\
& -3a_{60}a_3a_{15}a_{69}a_{52} + 2ia_{61}a_{44}a_4a_1a_{69}a_{52} - 2ia_{30}a_{32}a_1^2a_{69}a_{52} \\
& +4ia_{60}a_{44}a_{15}a_{37}a_{52} + 2a_{60}a_3a_{15}a_{37}a_{52} - ia_{61}a_{32}a_4a_1a_{37}a_{52} \\
& -a_{61}a_3a_4a_1a_{37}a_{52} - 2ia_{30}a_{32}a_1^2a_{37}a_{52} - a_{24}a_3a_1^2a_{73}a_{52} \\
& +12ia_{29}a_{32}a_{15}a_{74} - 8a_{29}a_3a_{15}a_{74} - 3ia_2a_{32}a_4a_1a_{74} + a_2a_3a_4a_1a_{74} \\
& -4a_{24}a_3a_1^2a_{74} - ia_{60}a_{44}a_{15}a_{69}a_{74} + 3a_{60}a_3a_{15}a_{69}a_{74} \\
& -2ia_{61}a_{32}a_4a_1a_{69}a_{74} + 2ia_{30}a_{32}a_1^2a_{69}a_{74} - 4ia_{60}a_{44}a_{15}a_{37}a_{74} \\
& -2a_{60}a_3a_{15}a_{37}a_{74} + ia_{61}a_{44}a_4a_1a_{37}a_{74} + a_{61}a_3a_4a_1a_{37}a_{74} \\
& +2ia_{30}a_{32}a_1^2a_{37}a_{74} - a_{24}a_3a_1^2a_{73}a_{74} - 18ia_{42}a_{44}a_{15}a_{59} - 2a_{42}a_3a_{15}a_{59} \\
& -4a_{34}a_3a_4a_1a_{59} - 4a_{41}a_3a_1^2a_{59} - ia_{67}a_{44}a_{15}a_{48}a_{59} + 3a_{67}a_3a_{15}a_{48}a_{59} \\
& -2ia_{70}a_{32}a_4a_1a_{48}a_{59} + 2ia_{45}a_{32}a_1^2a_{48}a_{59} - 5ia_{67}a_{44}a_{15}a_{37}a_{59} \\
& +a_{67}a_3a_{15}a_{37}a_{59} - ia_{70}a_{32}a_4a_1a_{37}a_{59} + a_{70}a_3a_4a_1a_{37}a_{59} \\
& -2ia_{45}a_{32}a_1^2a_{37}a_{59} + a_{41}a_3a_1^2a_{68}a_{59}\big)
\end{aligned}$$

where

$$a_1 := (1+3\sqrt{3}i)^{1/3}\,,\ a_2 := 2^{19/21}\,,\ a_3 := 3^{6/7}\,,\ a_4 := 7^{2/3}\,,\ a_5 := 29\,,$$

$$a_6 := 7^{7/3}\,,\ a_7 := 2(14^{1/3})\,,\ a_8 := 13 - 119\sqrt{3}i\,,\ a_9 := (2+6\sqrt{3}i)^{2/3}\,,$$

$$a_{10} := \overline{a_8}\,,\ a_{11} := 21922i\,,\ a_{12} := 1029\,,\ a_{13} := 700\,,\ a_{14} := 3290\,,$$

$$a_{15} := 7^{1/3}\,,\ a_{16} := 2^{2/3}\,,\ a_{17} := -a_1^3\,,\ a_{18} := (14+42\sqrt{3}i)^{1/3}\,,$$

$$a_{19} := \sqrt{\frac{6[14a_1^2 + a_{15}(-a_{16}a_1^3 - 2a_{18})]}{a_1^2}}\,,$$

$$a_{20} := 5 + \sqrt{3}i\,,\ a_{21} := 1 + \sqrt{3}i\,,\ a_{22} := \overline{a_{21}}\,,\ a_{23} := \sqrt{3} + 2i\,,\ a_{24} := 2^{4/7}\,,$$

$$a_{25} := \sqrt{\frac{6[14a_1^2 + a_{15}(a_{16}a_{20} + a_{21}a_{18})]}{a_1^2}}\,,$$

$$a_{26} := \sqrt{\frac{6[14a_1^2 + a_{15}(a_{22}a_{18} + 2ia_{16}a_{23})]}{a_1^2}}\,,$$

$$a_{27} := a_{12}a_{19} - a_{13}a_{25} - a_{14}a_{26}\,,\ a_{28} := -a_{11} + a_{27}\,,\ a_{29} := 2^{5/21}\,,\ a_{30} := 2^{1/14}\,,$$

$$a_{31} := \sqrt[7]{\frac{1}{a_1}\left[a_5\left(a_6(a_7a_8 + a_9a_{10}) - 2ia_1a_{28}\right)\right]}\,,$$

$$a_{32} := 3^{5/14}\,,\ a_{33} := a_{11} + a_{27}\,,\ a_{34} := 2^{1/21}\,,\ a_{35} := 86 - 33\sqrt{3}i\,,\ a_{36} := \overline{a_{35}}\,,$$

$$a_{37} := \sqrt{\frac{14a_1^2 + a_{15}(a_{22}a_{18} + 2ia_{16}a_{23})}{a_1^2}}\,,$$

$$a_{38} := \sqrt[7]{\frac{1}{a_1}\left[a_5\left(a_6(a_7a_8 + a_9a_{10}) + 2ia_1a_{33}\right)\right]}\,,$$

$$a_{39} := a_{13}a_{19} - a_{14}a_{25} - a_{12}a_{26}\,,\ a_{40} := a_{11} + a_{39}\,,\ a_{41} := 2^{5/7}\,,\ a_{42} := 2^{8/21}\,,$$

$$a_{43} := \sqrt[7]{\frac{1}{a_1}\left[a_5\left(a_6(a_9a_{35} + a_7a_{36}) + ia_1a_{40}\right)\right]}\,,$$

$$a_{44} := 3^{5/14}\,,\ a_{45} := 2^{3/14}\,,\ a_{46} := 29i\,,\ a_{47} := -53\sqrt{3} + 185i\,,$$

$$a_{48} := \sqrt{\frac{14a_1^2 - a_{15}(a_{16}a_1^3 + 2a_{18})}{a_1^2}}\,,$$

$$a_{49} := 53\sqrt{3} + 185i\,,\ a_{50} := a_{14}a_{19} - a_{12}a_{25} - a_{13}a_{26}\,,\ a_{51} := -a_{11} + a_{50}\,,$$

$$a_{52} := \sqrt[7]{-\frac{1}{a_1}\left[a_{46}\left(-a_6(a_{47}a_9 + a_7a_{49}) + 2a_1a_{51}\right)\right]}\,,$$

$$a_{53} := a_{11} + a_{50}\,,\ a_{54} := 21922\,,\ a_{55} := -ia_{39}\,,\ a_{56} := -a_{54} + a_{55}\,,\ a_{57} := 144\,,$$

$$a_{58} := \sqrt[7]{\frac{1}{a_1}\left[a_{46}\left(-a_6(a_{47}a_9 + a_7a_{49}) + 2a_1a_{53}\right)\right]}\,,$$

$$a_{59} := \sqrt[7]{\frac{1}{a_1}\left[a_5\left(a_6(a_9a_{35} + a_7a_{36}) + a_1a_{56}\right)\right]}\,,$$

$$a_{60} := 2^{31/42}\,,\ a_{61} := 2^{17/42}\,,\ a_{62} := 14a_1^2\,,\ a_{63} := a_{15}(a_{16}a_1^3 + 2a_{18})\,,$$

$$a_{64} := a_{62} - a_{63}\,,\; a_{65} := a_{15}(a_{22}a_{18} + 2ia_{16}a_{23})\,,\; a_{66} := a_{62} + a_{65}\,,\; a_{67} := 2^{37/42}\,,$$

$$a_{68} := \sqrt{\frac{a_{64}a_{66}}{a_1^4}}\,,\; a_{69} := \sqrt{\frac{14a_1^2 + a_{15}(a_{16}a_{20} + a_{21}a_{18})}{a_1^2}}\,,$$

$$a_{70} := 2^{23/42}\,,\; a_{71} := a_{15}(a_{16}a_{20} + a_{21}a_{18})\,,\; a_{72} := a_{62} + a_{71}\,,$$

$$a_{73} := \sqrt{\frac{a_{72}a_{66}}{a_1^4}}\,,\; a_{74} := \sqrt[7]{\frac{1}{a_1}\left[a_{46}\left(a_6(a_{47}a_9 + a_7a_{49}) + 2a_1a_{53}\right)\right]}\,.$$

Bibliography

[D] D. S. Dummit, *Solving Solvable Quintics*, Mathematics of Computation, Volume 57, Issue 195, 387-401, 1991.

[DF] D. S. Dummit & Richard M. Foote, *Abstract Algebra*, Prentice Hall, 1999.

[E] J.-P. Escofier, *Galois Theory*, Springer-Verlag, 2002.

[H] T. R. Hagedorn, *General Formulas for Solving Solvable Sextic Equations*, Journal of Algebra, Volume 233, Issue 2, 704-757, 2000.

[I] I. M. Isaacs, *Solution of Polynomials by Real Radicals*, The American Mathematical Monthly, Volume 92, Issue 8, 571-575, 1985.

[K] R. B. King, Beyond the Quartic Equation, Birkhäuser, 1996.

[KN] S. Kobayashi & H. Nakagawa, *Resolution of solvable quintic equation*, Mathematica Japonica, Volume 37, Issue 5, 1992.

[L] S. Lang, *Algebra*, Springer-Verlag, 2002.

[PS] V. Prasolov and Y. Solovgev, *Elliptic Functions and Elliptic Integrals*, American Mathematical Theory, 1977.

[R1] J. J. Rotman, *An Introduction to the Theory of Groups*, Springer-Verlag, 1994.

[R2] J. J. Rotman, *Galois Theory*, Springer-Verlag, 1990.

[SW] B. Spearman and K. S. Williams *On solvable Quintics* $x^5 + ax + b$ *and* $x^5 + ax^2 + b$, Rocky Mountain Journal of Mathematics, Volume 26, Number 2, 753-772, 1996.

[T] J.-P. Tignol, *Galois' Theory of Algebraic Equations*, World Scientific, 2001.

[V] T. M. Bŏsel, *http://www.vimagic.de/hope/index.html?/hope/inhalt.html*, University of Adelaide, 2002.

[W] E. Weisstein, *Eric Weisstein's World of Mathematics*, http://mathworld.wolfram.com/QuinticEquation.html

Appendix A

Solution of Polynomials by Real Radicals

In section 1.3, we have considered the following problem: Given a solvable polynomial with all its roots real, what are the necessary and sufficient conditions for one of the roots to be completely expressible in real radicals? Necessity is resolved affirmatively by the key result in [I] and we shall give an alternative proof of it here.

We shall first make the notion of real radical element precise.

Definition A.1. *Define $\alpha \in \mathbb{R}$ to be a real radical element if it lies in some repeated radical extension of $\mathbb{Q}$ that is contained in $\mathbb{R}$.*

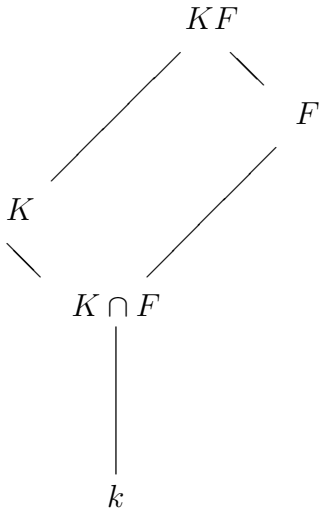
We quote the following result from [L] without proof.

Theorem A.2. (*natural irrationalities*) *Let K be a Galois extension of k, let F be an arbitrary extension and assume that K, F are subfields of some other field. Then the compositum KF is Galois over F, and K is Galois over $K \cap F$. Let H be the Galois group of KF over F, and G the Galois group of K over k. If $\sigma \in H$ then the restriction of σ to K is in G, and the map*

$$\sigma \mapsto \sigma|_K$$

gives an isomorphism of H on the Galois group of K over $K \cap F$. In partic-

ular, $[KF : F] = [K : K \cap F]$.



We will need the following lemma to prove the main theorem of this section.

Lemma A.3. *Let* k *and* $k[\gamma]$ *be subfields of* $\mathbb{R}$ *such that* $\gamma^n \in k$ *for some* $n \geq 0$. *Denote the normal closure of* $k[\gamma]$ *over* k *by* K. *If* $K \subseteq \mathbb{R}$, *then* $[k[\gamma] : k] \leq [K : k] \leq 2$.

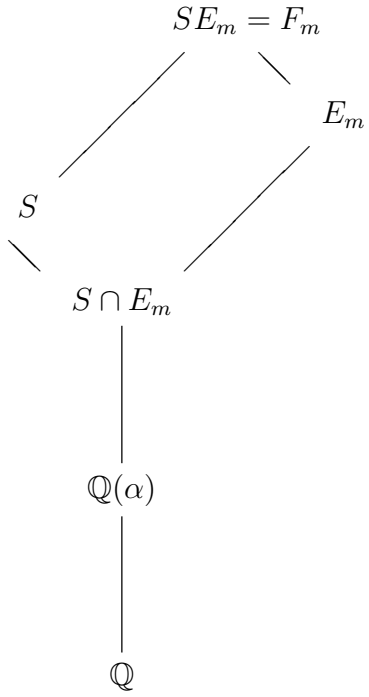
Proof. Let $m(x)$ be the minimal polynomial of γ over k. For $\sigma \in Gal(K/k)$,

$$(\gamma^\sigma)^n = (\gamma^n)^\sigma = \gamma^n \,,$$

and so $\gamma^\sigma = \gamma\zeta$ where $\zeta \in K$ is some nth root of unity. $K \subseteq \mathbb{R}$ forces $\zeta = \pm 1$ and thus $\gamma^\sigma = \pm\gamma$ for every element $\sigma \in Gal(K/k)$. Since the action of $Gal(K/k)$ on the roots of $m(x)$ is transitive, it follows that $\pm\gamma$ are the only possible conjugates of γ over k. Hence $m(x)$ being separable over k implies $[K : k] \leq 2!$ as desired. □

Theorem A.4. *Suppose* $f(x) \in \mathbb{Q}[x]$ *is an irreducible polynomial which splits over* $\mathbb{R}$. *If* $f(x)$ *has any root which is a real radical element, then the degree of* $f(x)$ *is a power of* 2 *and the Galois group of* $f(x)$ *over* $\mathbb{Q}$ *is a* 2*-group.*

Proof.



Let α be the real radical element with $f(\alpha) = 0$ and $S \subseteq \mathbb{R}$ be the splitting field for $f(x)$. By hypothesis, there exists a tower of fields

$$\mathbb{Q} = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_m$$

with $E_j = E_{j-1}[\gamma_j]$ such that $\gamma_j^{n_j} \in E_{j-1}$ for some $n_j \geq 0$ for all $1 \leq j \leq m$. Without loss of generality, we may assume $\alpha \in E_m - E_{m-1}$. For $1 \leq j \leq m$, let F_j denote the normal closure of E_j over E_{j-1}. Since $deg[f(x)]$ divides $[S : \mathbb{Q}] = |Gal(S/\mathbb{Q})|$ and $[S : \mathbb{Q}]$ divides $[SE_m : \mathbb{Q}]$, it suffices to show that $[SE_m : \mathbb{Q}]$ is a power of 2.

We first claim that $SE_m = F_m$. Because F_m is normal over E_{m-1}, F_m is also normal over $\mathbb{Q}(\alpha)$. Thus $S \subseteq F_m$ and $SE_m \subseteq F_m$. On the other hand, by natural irrationalities applied to S and E_m, SE_m is Galois over E_m. Therefore $F_m \subseteq SE_m$ and so $SE_m = F_m$ as claimed.

Note that S being normal over $\mathbb{Q}$ is also normal over E_j for $1 \leq j \leq m-1$. Consequently, $F_j \subseteq S \subseteq \mathbb{R}$ for all $1 \leq jm - 1$. Also S, $E_m \subseteq \mathbb{R}$ implies $F_m = SE_m \subseteq \mathbb{R}$. Hence applying Lemma $A.3$ by taking $k = E_{j-1}$, $\gamma = \gamma_j$, $n = n_j$ for each $1 \leq j \leq m$ yields $[E_j : E_{j-1}] \leq 2$ for all $1 \leq j \leq m-1$ and $[F_m : E_{m-1}] \leq 2$. Therefore

$$[F_m : \mathbb{Q}] = [F_m : E_{m-1}] \prod_{j=1}^{m-1} [E_j : E_{j-1}] = 2^u$$

for some $u \leq m$ as required. $\square$

Appendix B

lagres.nb

Collect[Expand[$(x_1 + x_2\zeta + x_3\zeta^2 + x_4\zeta^3 + x_5\zeta^4 + x_6\zeta^5 + x_7\zeta^6)^7$] /. $\zeta \to$ Exp[2 * Pi * I / 7], Exp[2 * Pi * I / 7]]

$x_1 = \omega + \omega^{12} + \omega^{28} + \omega^{17}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_2 = \omega^2 + \omega^{24} + \omega^{27} + \omega^5$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_3 = \omega^4 + \omega^{19} + \omega^{25} + \omega^{10}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_4 = \omega^8 + \omega^9 + \omega^{21} + \omega^{20}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_5 = \omega^{16} + \omega^{18} + \omega^{13} + \omega^{11}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_6 = \omega^3 + \omega^7 + \omega^{26} + \omega^{22}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_7 = \omega^6 + \omega^{14} + \omega^{23} + \omega^{15}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
Simplify[$l_0[x_{1\_}, x_{2\_}, x_{3\_}, x_{4\_}, x_{5\_}, x_{6\_}, x_{7\_}] \to \hat{l_0}$ [1]]
$x_1 = \omega + \omega^{12} + \omega^{28} + \omega^{17}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_2 = \omega^2 + \omega^{24} + \omega^{27} + \omega^5$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_3 = \omega^4 + \omega^{19} + \omega^{25} + \omega^{10}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_4 = \omega^8 + \omega^9 + \omega^{21} + \omega^{20}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_5 = \omega^{16} + \omega^{18} + \omega^{13} + \omega^{11}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_6 = \omega^3 + \omega^7 + \omega^{26} + \omega^{22}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_7 = \omega^6 + \omega^{14} + \omega^{23} + \omega^{15}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
Simplify[$l_1[x_{1\_}, x_{2\_}, x_{3\_}, x_{4\_}, x_{5\_}, x_{6\_}, x_{7\_}] \to \hat{l_1}$]

$x_1 = \omega + \omega^{12} + \omega^{28} + \omega^{17}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_2 = \omega^2 + \omega^{24} + \omega^{27} + \omega^5$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_3 = \omega^4 + \omega^{19} + \omega^{25} + \omega^{10}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_4 = \omega^8 + \omega^9 + \omega^{21} + \omega^{20}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_5 = \omega^{16} + \omega^{18} + \omega^{13} + \omega^{11}$ /. $\omega \to$ Exp[2 * Pi * I / 29]

[1] In practice, we shall use the cut and paste commands from the output of the first command to generate the symbolic expressions for l_j which we denote by $\hat{l_j}$, $0 \leq j \leq 6$.

$x_6 = \omega^3 + \omega^7 + \omega^{26} + \omega^{22}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_7 = \omega^6 + \omega^{14} + \omega^{23} + \omega^{15}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
Simplify[$l_3[x_{1\_}, x_{2\_}, x_{3\_}, x_{4\_}, x_{5\_}, x_{6\_}, x_{7\_}] \to \hat{l_3}$]
$x_1 = \omega + \omega^{12} + \omega^{28} + \omega^{17}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_2 = \omega^8 + \omega^9 + \omega^{21} + \omega^{20}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_3 = \omega^6 + \omega^{14} + \omega^{23} + \omega^{15}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_4 = \omega^4 + \omega^{19} + \omega^{25} + \omega^{10}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_5 = \omega^3 + \omega^7 + \omega^{26} + \omega^{22}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_6 = \omega^2 + \omega^{24} + \omega^{27} + \omega^5$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_7 = \omega^{16} + \omega^{18} + \omega^{13} + \omega^{11}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
Simplify[$l_1[x_{1\_}, x_{2\_}, x_{3\_}, x_{4\_}, x_{5\_}, x_{6\_}, x_{7\_}] \to \hat{l_1}$]

$x_1 = \omega + \omega^{12} + \omega^{28} + \omega^{17}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_2 = \omega^2 + \omega^{24} + \omega^{27} + \omega^5$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_3 = \omega^4 + \omega^{19} + \omega^{25} + \omega^{10}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_4 = \omega^8 + \omega^9 + \omega^{21} + \omega^{20}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_5 = \omega^{16} + \omega^{18} + \omega^{13} + \omega^{11}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_6 = \omega^3 + \omega^7 + \omega^{26} + \omega^{22}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_7 = \omega^6 + \omega^{14} + \omega^{23} + \omega^{15}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
Simplify[$l_2[x_{1\_}, x_{2\_}, x_{3\_}, x_{4\_}, x_{5\_}, x_{6\_}, x_{7\_}] \to \hat{l_2}$]
$x_1 = \omega + \omega^{12} + \omega^{28} + \omega^{17}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_2 = \omega^4 + \omega^{19} + \omega^{25} + \omega^{10}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_3 = \omega^{16} + \omega^{18} + \omega^{13} + \omega^{11}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_4 = \omega^6 + \omega^{14} + \omega^{23} + \omega^{15}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_5 = \omega^2 + \omega^{24} + \omega^{27} + \omega^5$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_6 = \omega^8 + \omega^9 + \omega^{21} + \omega^{20}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_7 = \omega^3 + \omega^7 + \omega^{26} + \omega^{22}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
Simplify[$l_1[x_{1\_}, x_{2\_}, x_{3\_}, x_{4\_}, x_{5\_}, x_{6\_}, x_{7\_}] \to \hat{l_1}$]

$x_1 = \omega + \omega^{12} + \omega^{28} + \omega^{17}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_2 = \omega^2 + \omega^{24} + \omega^{27} + \omega^5$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_3 = \omega^4 + \omega^{19} + \omega^{25} + \omega^{10}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_4 = \omega^8 + \omega^9 + \omega^{21} + \omega^{20}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_5 = \omega^{16} + \omega^{18} + \omega^{13} + \omega^{11}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_6 = \omega^3 + \omega^7 + \omega^{26} + \omega^{22}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_7 = \omega^6 + \omega^{14} + \omega^{23} + \omega^{15}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
Simplify[$l_6[x_{1\_}, x_{2\_}, x_{3\_}, x_{4\_}, x_{5\_}, x_{6\_}, x_{7\_}] \to \hat{l_6}$]
$x_1 = \omega + \omega^{12} + \omega^{28} + \omega^{17}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_2 = \omega^6 + \omega^{14} + \omega^{23} + \omega^{15}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_3 = \omega^3 + \omega^7 + \omega^{26} + \omega^{22}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_4 = \omega^{16} + \omega^{18} + \omega^{13} + \omega^{11}$ /. $\omega \to$ Exp[2 * Pi * I / 29]

$x_5 = \omega^8 + \omega^9 + \omega^{21} + \omega^{20}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_6 = \omega^4 + \omega^{19} + \omega^{25} + \omega^{10}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_7 = \omega^2 + \omega^{24} + \omega^{27} + \omega^5$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$\text{Simplify}[l_1[x_{1\_}, x_{2\_}, x_{3\_}, x_{4\_}, x_{5\_}, x_{6\_}, x_{7\_}] \to \hat{l_1}]$

$x_1 = \omega + \omega^{12} + \omega^{28} + \omega^{17}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_2 = \omega^2 + \omega^{24} + \omega^{27} + \omega^5$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_3 = \omega^4 + \omega^{19} + \omega^{25} + \omega^{10}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_4 = \omega^8 + \omega^9 + \omega^{21} + \omega^{20}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_5 = \omega^{16} + \omega^{18} + \omega^{13} + \omega^{11}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_6 = \omega^3 + \omega^7 + \omega^{26} + \omega^{22}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_7 = \omega^6 + \omega^{14} + \omega^{23} + \omega^{15}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$\text{Simplify}[l_4[x_{1\_}, x_{2\_}, x_{3\_}, x_{4\_}, x_{5\_}, x_{6\_}, x_{7\_}] \to \hat{l_4}]$
$x_1 = \omega + \omega^{12} + \omega^{28} + \omega^{17}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_2 = \omega^{16} + \omega^{18} + \omega^{13} + \omega^{11}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_3 = \omega^2 + \omega^{24} + \omega^{27} + \omega^5$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_4 = \omega^3 + \omega^7 + \omega^{26} + \omega^{22}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_5 = \omega^4 + \omega^{19} + \omega^{25} + \omega^{10}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_6 = \omega^6 + \omega^{14} + \omega^{23} + \omega^{15}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_7 = \omega^8 + \omega^9 + \omega^{21} + \omega^{20}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$\text{Simplify}[l_1[x_{1\_}, x_{2\_}, x_{3\_}, x_{4\_}, x_{5\_}, x_{6\_}, x_{7\_}] \to \hat{l_1}]$

$x_1 = \omega + \omega^{12} + \omega^{28} + \omega^{17}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_2 = \omega^2 + \omega^{24} + \omega^{27} + \omega^5$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_3 = \omega^4 + \omega^{19} + \omega^{25} + \omega^{10}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_4 = \omega^8 + \omega^9 + \omega^{21} + \omega^{20}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_5 = \omega^{16} + \omega^{18} + \omega^{13} + \omega^{11}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_6 = \omega^3 + \omega^7 + \omega^{26} + \omega^{22}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_7 = \omega^6 + \omega^{14} + \omega^{23} + \omega^{15}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$\text{Simplify}[l_5[x_{1\_}, x_{2\_}, x_{3\_}, x_{4\_}, x_{5\_}, x_{6\_}, x_{7\_}] \to \hat{l_5}]$
$x_1 = \omega + \omega^{12} + \omega^{28} + \omega^{17}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_2 = \omega^3 + \omega^7 + \omega^{26} + \omega^{22}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_3 = \omega^8 + \omega^9 + \omega^{21} + \omega^{20}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_4 = \omega^2 + \omega^{24} + \omega^{27} + \omega^5$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_5 = \omega^6 + \omega^{14} + \omega^{23} + \omega^{15}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_6 = \omega^{16} + \omega^{18} + \omega^{13} + \omega^{11}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_7 = \omega^4 + \omega^{19} + \omega^{25} + \omega^{10}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$\text{Simplify}[l_1[x_{1\_}, x_{2\_}, x_{3\_}, x_{4\_}, x_{5\_}, x_{6\_}, x_{7\_}] \to \hat{l_1}]$

$x_1 = \omega + \omega^{12} + \omega^{28} + \omega^{17}$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$
$x_2 = \omega^2 + \omega^{24} + \omega^{27} + \omega^5$ /. $\omega \to \text{Exp}[2 * \text{Pi} * \text{I} / 29]$

$x_3 = \omega^4 + \omega^{19} + \omega^{25} + \omega^{10}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_4 = \omega^8 + \omega^9 + \omega^{21} + \omega^{20}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_5 = \omega^{16} + \omega^{18} + \omega^{13} + \omega^{11}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_6 = \omega^3 + \omega^7 + \omega^{26} + \omega^{22}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$x_7 = \omega^6 + \omega^{14} + \omega^{23} + \omega^{15}$ /. $\omega \to$ Exp[2 * Pi * I / 29]
$\zeta =$ Exp[2 * Pi * I / 7]
$R_1 = 8352\zeta - 986\zeta^2 + 108634\zeta^3 + 78793\zeta^4 + 19314\zeta^5 + 103762\zeta^6$
$R_2 = 78793\zeta + 8352\zeta^2 + 19314\zeta^3 - 986\zeta^4 + 103762\zeta^5 + 108634\zeta^6$
$R_3 = 19314\zeta + 108634\zeta^2 + 8352\zeta^3 + 103762\zeta^4 + 78793\zeta^5 - 986\zeta^6$
$R_4 = -986\zeta + 78793\zeta^2 + 103762\zeta^3 + 8352\zeta^4 + 108634\zeta^5 + 19314\zeta^6$
$R_5 = 108634\zeta + 103762\zeta^2 - 986\zeta^3 + 19314\zeta^4 + 8352\zeta^5 + 78793\zeta^6$
$R_6 = 103762\zeta + 19314\zeta^2 + 78793\zeta^3 + 108634\zeta^4 - 986\zeta^5 + 8352\zeta^6$
Lr[z_] := $x_1 + x_2 z + x_3 z^2 + x_4 z^3 + x_5 z^4 + x_6 z^5 + x_7 z^6$
For[$j = 1,\ j < 7,\ j++,\ n_j =$ N[(7 * Arg [Lr[ζ^j]]-Arg [R_j])/(2 * Pi), 400];
Print[n_j]]

$$a = \frac{1}{2}\left(-\frac{1}{3} + \frac{7^{2/3}}{3(\frac{1}{2}(1+3i\sqrt{3}))^{1/3}} + \frac{1}{3}\left(\frac{7}{2}(1+3i\sqrt{3})\right)^{1/3}\right) +$$

$$i\left(\frac{1}{2}\sqrt{\frac{14(1+3i\sqrt{3})^{2/3} + 7^{1/3}((1-i\sqrt{3})(14+42i\sqrt{3})^{1/3} + 2i2^{2/3}(2i+\sqrt{3}))}{6(1+3i\sqrt{3})^{2/3}}}\right)$$

$$b = \frac{1}{2}\left(-\frac{1}{3} - \frac{(\frac{7}{2})^{2/3}(1-i\sqrt{3})}{3(1+3i\sqrt{3})^{1/3}} - \frac{1}{6}(1+i\sqrt{3})\left(\frac{7}{2}(1+3i\sqrt{3})\right)^{1/3}\right) +$$

$$i\left(\frac{1}{2}\sqrt{\frac{14(1+3i\sqrt{3})^{2/3} + 7^{1/3}(2^{2/3}(5+i\sqrt{3})^{1/3} + (1+i\sqrt{3})(14+42i\sqrt{3})^{1/3})}{6(1+3i\sqrt{3})^{2/3}}}\right)$$

$$c = \frac{1}{2}\left(-\frac{1}{3} - \frac{(\frac{7}{2})^{2/3}(1+i\sqrt{3})}{3(1+3i\sqrt{3})^{1/3}} - \frac{1}{6}(1-i\sqrt{3})\left(\frac{7}{2}(1+3i\sqrt{3})\right)^{1/3}\right) +$$
$$i\left(\frac{1}{2}\sqrt{\frac{14(1+3i\sqrt{3})^{2/3} - 7^{1/3}(2^{2/3}(1+3i\sqrt{3}) + 2(14+42i\sqrt{3})^{1/3})}{6(1+3i\sqrt{3})^{2/3}}}\right)$$
$$d = \frac{1}{2}\left(-\frac{1}{3} - \frac{(\frac{7}{2})^{2/3}(1+i\sqrt{3})}{3(1+3i\sqrt{3})^{1/3}} - \frac{1}{6}(1-i\sqrt{3})\left(\frac{7}{2}(1+3i\sqrt{3})\right)^{1/3}\right) -$$
$$i\left(\frac{1}{2}\sqrt{\frac{14(1+3i\sqrt{3})^{2/3} - 7^{1/3}(2^{2/3}(1+3i\sqrt{3}) + 2(14+42i\sqrt{3})^{1/3})}{6(1+3i\sqrt{3})^{2/3}}}\right)$$

$$e = \frac{1}{2}\left(-\frac{1}{3} - \frac{(\frac{7}{2})^{2/3}(1-i\sqrt{3})}{3(1+3i\sqrt{3})^{1/3}} - \frac{1}{6}(1+i\sqrt{3})\left(\frac{7}{2}(1+3i\sqrt{3})\right)^{1/3}\right) -$$

$$i\left(\frac{1}{2}\sqrt{\frac{14(1+3i\sqrt{3})^{2/3} + 7^{1/3}(2^{2/3}(5+i\sqrt{3})^{1/3} + (1+i\sqrt{3})(14+42i\sqrt{3})^{1/3})}{6(1+3i\sqrt{3})^{2/3}}}\right)$$

$$f = \frac{1}{2}\left(-\frac{1}{3} + \frac{7^{2/3}}{3(\frac{1}{2}(1+3i\sqrt{3}))^{1/3}} + \frac{1}{3}\left(\frac{7}{2}(1+3i\sqrt{3})\right)^{1/3}\right) -$$

$$i\left(\frac{1}{2}\sqrt{\frac{14(1+3i\sqrt{3})^{2/3} + 7^{1/3}((1-i\sqrt{3})(14+42i\sqrt{3})^{1/3} + 2i2^{2/3}(2i+\sqrt{3}))}{6(1+3i\sqrt{3})^{2/3}}}\right)$$

$\text{Simplify}[\text{Expand}[R_1 = 8352a - 986b + 108634c + 78793d + 19314e + 103762f]]$
$\text{Simplify}[\text{Expand}[R_2 = 78793a + 8352b + 19314c - 986d + 103762e + 108634f]]$
$\text{Simplify}[\text{Expand}[R_3 = 19314a + 108634b + 8352c + 103762d + 78793e - 986f]]$
$\text{Simplify}[\text{Expand}[R_4 = -986a + 78793b + 103762c + 8352d + 108634e + 19314f]]$
$\text{Simplify}[\text{Expand}[R_5 = 108634a + 103762b - 986c + 19314d + 8352e + 78793f]]$
$\text{Simplify}[\text{Expand}[R_6 = 103762a + 19314b + 78793c + 108634d - 986e + 8352f]]$

$\text{Simplify}[\text{Expand}[r_1 = a\sqrt[7]{(R_1)}]]$
$\text{Simplify}[\text{Expand}[r_2 = c\sqrt[7]{(R_2)}]]$
$\text{Simplify}[\text{Expand}[r_3 = a\sqrt[7]{(R_3)}]]$
$\text{Simplify}[\text{Expand}[r_4 = f\sqrt[7]{(R_4)}]]$
$\text{Simplify}[\text{Expand}[r_5 = d\sqrt[7]{(R_5)}]]$
$\text{Simplify}[\text{Expand}[r_6 = f\sqrt[7]{(R_6)}]]$

$x_1 = \text{Simplify}[\text{Expand}[(1/7) * (-1 + r_1 + r_2 + r_3 + r_4 + r_5 + r_6)]]$
$x_5 = \text{Simplify}[\text{Expand}[(1/7) * (-1 + c * r_1 + f * r_2 + b * r_3 + e * r_4 + a * r_5 + d * r_6)]]$

$c = \text{Simplify}[\text{Expand}[(1/4) * (x_1 + \sqrt{(x_1)^2 - 4x_5})]]$

Explicitly,

$$
\begin{aligned}
l_1 \;=\;& 7x_1^6x_2 + 7x_2^6x_3 + 105x_1x_2^4x_3^2 + 210x_1^2x_2^2x_3^3 + 35x_1^3x_3^4 + 42x_1x_2^5x_4 \\
&+420x_1^2x_2^3x_3x_4 + 420x_1^3x_2x_3^2x_4 + 7x_3^6x_4 + 210x_1^3x_2^2x_4^2 + 105x_1^4x_3x_4^2 \\
&+105x_2x_3^4x_4^2 + 210x_2^2x_3^2x_4^3 + 140x_1x_3^3x_4^3 + 35x_2^3x_4^4 + 210x_1x_2x_3x_4^4 \\
&+21x_1^2x_4^5 + 105x_1^2x_2^4x_5 + 420x_1^3x_2^2x_3x_5 + 105x_1^4x_3^2x_5 + 42x_2x_3^5x_5 \\
&+210x_1^4x_2x_4x_5 + 420x_2^2x_3^3x_4x_5 + 210x_1x_3^4x_4x_5 + 420x_2^3x_3x_4^2x_5 \\
&+1260x_1x_2x_3^2x_4^2x_5 + 420x_1x_2^2x_4^3x_5 + 420x_1^2x_3x_4^3x_5 + 7x_4^6x_5 + 21x_1^5x_5^2 \\
&+210x_2^3x_3^2x_5^2 + 420x_1x_2x_3^3x_5^2 + 105x_2^4x_4x_5^2 + 1260x_1x_2^2x_3x_4x_5^2 \\
&+630x_1^2x_3^2x_4x_5^2 + 630x_1^2x_2x_4^2x_5^2 + 105x_3x_4^4x_5^2 + 140x_1x_2^3x_5^3 \\
&+420x_1^2x_2x_3x_5^3 + 140x_1^3x_4x_5^3 + 210x_3^2x_4^2x_5^3 + 140x_2x_4^3x_5^3 + 35x_3^3x_5^4 \\
&+210x_2x_3x_4x_5^4 + 105x_1x_4^2x_5^4 + 21x_2^2x_5^5 + 42x_1x_3x_5^5 + 140x_1^3x_2^3x_6 \\
&+210x_1^4x_2x_3x_6 + 105x_2^2x_3^4x_6 + 42x_1x_3^5x_6 + 42x_1^5x_4x_6 + 420x_2^3x_3^2x_4x_6 \\
&+840x_1x_2x_3^3x_4x_6 + 105x_2^4x_4^2x_6 + 1260x_1x_2^2x_3x_4^2x_6 + 630x_1^2x_3^2x_4^2x_6 \\
&+420x_1^2x_2x_4^3x_6 + 42x_3x_4^5x_6 + 210x_2^4x_3x_5x_6 + 1260x_1x_2^2x_3^2x_5x_6 \\
&+420x_1^2x_3^3x_5x_6 + 840x_1x_2^3x_4x_5x_6 + 2520x_1^2x_2x_3x_4x_5x_6 + 420x_1^3x_4^2x_5x_6 \\
&+420x_3^2x_4^3x_5x_6 + 210x_2x_4^4x_5x_6 + 630x_1^2x_2^2x_5^2x_6 + 420x_1^3x_3x_5^2x_6 \\
&+420x_3^3x_4x_5^2x_6 + 1260x_2x_3x_4^2x_5^2x_6 + 420x_1x_4^3x_5^2x_6 + 420x_2x_3^2x_5^3x_6 \\
&+420x_2^2x_4x_5^3x_6 + 840x_1x_3x_4x_5^3x_6 + 210x_1x_2x_5^4x_6 + 7x_5^6x_6 + 21x_2^5x_6^2 \\
&+420x_1x_2^3x_3x_6^2 + 630x_1^2x_2x_3^2x_6^2 + 630x_1^2x_2^2x_4x_6^2 + 420x_1^3x_3x_4x_6^2 \\
&+210x_3^3x_4^2x_6^2 + 420x_2x_3x_4^3x_6^2 + 105x_1x_4^4x_6^2 + 420x_1^3x_2x_5x_6^2 + 105x_3^4x_5x_6^2 \\
&+1260x_2x_3^2x_4x_5x_6^2 + 630x_2^2x_4^2x_5x_6^2 + 1260x_1x_3x_4^2x_5x_6^2 + 630x_2^2x_3x_5^2x_6^2 \\
&+630x_1x_3^2x_5^2x_6^2 + 1260x_1x_2x_4x_5^2x_6^2 + 210x_1^2x_5^3x_6^2 + 105x_4x_5^4x_6^2 \\
&+35x_1^4x_6^3 + 140x_2x_3^3x_6^3 + 420x_2^2x_3x_4x_6^3 + 420x_1x_3^2x_4x_6^3 + 420x_1x_2x_4^2x_6^3 \\
&+140x_2^3x_5x_6^3 + 840x_1x_2x_3x_5x_6^3 + 420x_1^2x_4x_5x_6^3 + 210x_4^2x_5^2x_6^3 \\
&+140x_3x_5^3x_6^3 + 105x_1x_2^2x_6^4 + 105x_1^2x_3x_6^4 + 35x_4^3x_6^4 + 210x_3x_4x_5x_6^4 \\
&+105x_2x_5^2x_6^4 + 21x_3^2x_6^5 + 42x_2x_4x_6^5 + 42x_1x_5x_6^5 + 105x_1^4x_2^2x_7 \\
&+42x_1^5x_3x_7 + 140x_2^3x_3^3x_7 + 210x_1x_2x_3^4x_7 + 210x_2^4x_3x_4x_7 \\
&+1260x_1x_2^2x_3^2x_4x_7 + 420x_1^2x_3^3x_4x_7 + 420x_1x_2^3x_4^2x_7 + 1260x_1^2x_2x_3x_4^2x_7 \\
&+140x_1^3x_4^3x_7 + 105x_3^2x_4^4x_7 + 42x_2x_4^5x_7 + 42x_2^5x_5x_7 + 840x_1x_2^3x_3x_5x_7 \\
&+1260x_1^2x_2x_3^2x_5x_7 + 1260x_1^2x_2^2x_4x_5x_7 + 840x_1^3x_3x_4x_5x_7 + 420x_3^3x_4^2x_5x_7 \\
&+840x_2x_3x_4^3x_5x_7 + 210x_1x_4^4x_5x_7 + 420x_1^3x_2x_5^2x_7 + 105x_3^4x_5^2x_7 \\
&+1260x_2x_3^2x_4x_5^2x_7 + 630x_2^2x_4^2x_5^2x_7 + 1260x_1x_3x_4^2x_5^2x_7 + 420x_2^2x_3x_5^3x_7 \\
&+420x_1x_3^2x_5^3x_7 + 840x_1x_2x_4x_5^3x_7 + 105x_1^2x_5^4x_7 + 42x_4x_5^5x_7 \\
&+210x_1x_2^4x_6x_7 + 1260x_1^2x_2^2x_3x_6x_7 + 420x_1^3x_3^2x_6x_7 + 840x_1^3x_2x_4x_6x_7 \\
&+210x_3^4x_4x_6x_7 + 1260x_2x_3^2x_4^2x_6x_7 + 420x_2^2x_4^3x_6x_7 + 840x_1x_3x_4^3x_6x_7
\end{aligned}
$$

$$
\begin{aligned}
&+210x_1^4x_5x_6x_7 + 840x_2x_3^3x_5x_6x_7 + 2520x_2^2x_3x_4x_5x_6x_7\\
&+2520x_1x_3^2x_4x_5x_6x_7 + 2520x_1x_2x_4^2x_5x_6x_7 + 420x_2^3x_5^2x_6x_7\\
&+2520x_1x_2x_3x_5^2x_6x_7 + 1260x_1^2x_4x_5^2x_6x_7 + 420x_4^2x_5^3x_6x_7 + 210x_3x_5^4x_6x_7\\
&+630x_2^2x_3^2x_6^2x_7 + 420x_1x_3^3x_6^2x_7 + 420x_2^3x_4x_6^2x_7 + 2520x_1x_2x_3x_4x_6^2x_7\\
&+630x_1^2x_4^2x_6^2x_7 + 1260x_1x_2^2x_5x_6^2x_7 + 1260x_1^2x_3x_5x_6^2x_7 + 420x_4^3x_5x_6^2x_7\\
&+1260x_3x_4x_5^2x_6^2x_7 + 420x_2x_5^3x_6^2x_7 + 420x_1^2x_2x_6^3x_7 + 420x_3x_4^2x_6^3x_7\\
&+420x_3^2x_5x_6^3x_7 + 840x_2x_4x_5x_6^3x_7 + 420x_1x_5^2x_6^3x_7 + 210x_2x_3x_6^4x_7\\
&+210x_1x_4x_6^4x_7 + 7x_6^6x_7 + 210x_1^2x_2^3x_7^2 + 420x_1^3x_2x_3x_7^2 + 21x_3^5x_7^2\\
&+105x_1^4x_4x_7^2 + 420x_2x_3^3x_4x_7^2 + 630x_2^2x_3x_4^2x_7^2 + 630x_1x_3^2x_4^2x_7^2\\
&+420x_1x_2x_4^3x_7^2 + 630x_2^2x_3^2x_5x_7^2 + 420x_1x_3^3x_5x_7^2 + 420x_2^3x_4x_5x_7^2\\
&+2520x_1x_2x_3x_4x_5x_7^2 + 630x_1^2x_4^2x_5x_7^2 + 630x_1x_2^2x_5^2x_7^2 + 630x_1^2x_3x_5^2x_7^2\\
&+210x_4^3x_5^2x_7^2 + 420x_3x_4x_5^3x_7^2 + 105x_2x_5^4x_7^2 + 420x_2^3x_3x_6x_7^2\\
&+1260x_1x_2x_3^2x_6x_7^2 + 1260x_1x_2^2x_4x_6x_7^2 + 1260x_1^2x_3x_4x_6x_7^2 + 105x_4^4x_6x_7^2\\
&+1260x_1^2x_2x_5x_6x_7^2 + 1260x_3x_4^2x_5x_6x_7^2 + 630x_3^2x_5^2x_6x_7^2 + 1260x_2x_4x_5^2x_6x_7^2\\
&+420x_1x_5^3x_6x_7^2 + 210x_1^3x_6^2x_7^2 + 630x_3^2x_4x_6^2x_7^2 + 630x_2x_4^2x_6^2x_7^2\\
&+1260x_2x_3x_5x_6^2x_7^2 + 1260x_1x_4x_5x_6^2x_7^2 + 210x_2^2x_6^3x_7^2 + 420x_1x_3x_6^3x_7^2\\
&+105x_5x_6^4x_7^2 + 35x_2^4x_7^3 + 420x_1x_2^2x_3x_7^3 + 210x_1^2x_3^2x_7^3 + 420x_1^2x_2x_4x_7^3\\
&+140x_3x_4^3x_7^3 + 140x_1^3x_5x_7^3 + 420x_3^2x_4x_5x_7^3 + 420x_2x_4^2x_5x_7^3 + 420x_2x_3x_5^2x_7^3\\
&+420x_1x_4x_5^2x_7^3 + 140x_3^3x_6x_7^3 + 840x_2x_3x_4x_6x_7^3 + 420x_1x_4^2x_6x_7^3\\
&+420x_2^2x_5x_6x_7^3 + 840x_1x_3x_5x_6x_7^3 + 420x_1x_2x_6^2x_7^3 + 210x_5^2x_6^2x_7^3 + 140x_4x_6^3x_7^3\\
&+105x_2x_3^2x_7^4 + 105x_2^2x_4x_7^4 + 210x_1x_3x_4x_7^4 + 210x_1x_2x_5x_7^4 + 35x_5^3x_7^4\\
&+105x_1^2x_6x_7^4 + 210x_4x_5x_6x_7^4 + 105x_3x_6^2x_7^4 + 21x_4^2x_7^5 + 42x_3x_5x_7^5\\
&+42x_2x_6x_7^5 + 7x_1x_7^6\,,
\end{aligned}
$$

$$
l_2 = (2,\ 3,\ 5)(4,\ 7,\ 6)l_1\,,\ l_3 = (2,\ 4,\ 3,\ 7,\ 5,\ 6)l_1\,,\ l_4 = (2,\ 5,\ 3)(4,\ 6,\ 7)l_1\,,
$$

$$
l_5 = (2,\ 6,\ 5,\ 7,\ 3,\ 4)l_1\,,\ l_6 = (2,\ 7)(4,\ 5)(3,\ 6)l_1\,,\ l_0 = s_1 - \sum_{j=1}^{6} l_j\,.
$$